INFORME FINAL

PROYECTO UTU –CETP

Alumno: Rosana Almada
Responsable: Oscar Camargo
Tutor: Alberto Pardo.
2003-2004

INDICE

ABSTRACT **1**

1 INTRODUCCIÓN **2**

1.1 DECLARACIONES JURADAS 2
1.2 OBJETIVO Y ALCANCE 3

2 ANÁLISIS DE REQUERIMIENTOS **5**

2.1 SISTEMA DE DECLARACIONES JURADAS 5
2.2 SISTEMA DE CONECTIVIDAD 6

3 DISEÑO **7**

3.1 DISEÑO SISTEMA DECLARACIONES JURADAS 7
3.1.1 Modelo Entidad Relación – Bedelía Informatizada Existente. *7*
3.1.2 Modelo Entidad Relación – Sistema Declaraciones Juradas. *9*
3.1.3 Especificación de Procesos *13*
3.2 PROPUESTAS DE DISEÑO DE CONECTIVIDAD 15

4 IMPLEMENTACIÓN **24**

4.1 SITUACIÓN ORGANIZACIONAL DE UTU 24
4.2 SISTEMA DE DECLARACIONES JURADAS 26
4.3 DECLARACIONES JURADAS - ESQUEMA DE PANTALLAS 26
4.3.1 Ingresar Declaraciones Juradas de esta Repartición *27*
4.3.2 Cursos Móviles *30*
4.3.3 Envío de datos hacia el CETP *31*

5 CONCLUSIONES **32**

6 PROYECCIONES A FUTURO **34**

APÉNDICE A: FORMULARIO DE DECLARACIONES JURADAS **35**

APÉNDICE B – DISEÑO DE BASE DE DATOS **37**

APÉNDICE C: FIREWALL **43**

APÉNDICE D - ZONA DESMILITARIZADA (DMZ) **49**

APÉNDICE E- REDES PRIVADAS VIRTUALES **51**

BIBLIOGRAFÍA **54**

Abstract

El problema de la integración de diferentes sistemas informáticos existentes en el Consejo de Educación Técnico Profesional ha sido un proyecto que se ha estado desarrollando durante los últimos años y que aún continúa. La centralización de información docente, que se encontraba en diferentes sistemas de forma repetida e inconsistente desencadena el problema referente a la designación de horas docentes que están involucradas al cobro de haberes de los funcionarios que dictan clases en las diferentes Reparticiones. El CETP ve entonces la necesidad de la integración de datos provenientes de las diferentes Reparticiones e insertarlas dentro del sistema de base de datos central lo más automáticamente posible, sin demoras en el traslado de los datos con niveles de seguridad y confiabilidad adecuados al tipo de datos que se manejan.

En este documento se presenta el diseño e implementación del sistema de Ingreso de Declaraciones Juradas correspondiente a las designaciones docentes y se proponen diferentes mecanismos de conectividad como soluciones viables para la transferencia de datos entre el CETP y las Escuelas Técnicas. La sección 1 describe una introducción sobre la realidad sobre la cual se desarrolla este proyecto. En la sección 2 se presenta el análisis de los requerimientos. La sección 3 establece el diseño propuesto para la implementación del sistema de ingreso de Declaraciones Juradas y de conectividad, para finalmente, en la sección 4 presentar la implementación desarrollada. En la Sección 5 y 6 se presentan las conclusiones y los desarrollos que aún quedan pendientes por resolver luego de la finalización del presente proyecto.

1 Introducción

1.1 Declaraciones Juradas

La Declaración Jurada es un formulario que cada docente debe completar al inicio de cada año lectivo, donde se refleja la situación laboral del mismo dentro y fuera de la enseñanza pública. En el apéndice A se encuentra una copia del formulario de Declaración Jurada.
Antes del comienzo de cada año lectivo, el CETP[1] libera un listado compuesto por las horas docentes existentes en cada una de las Escuelas UTU[2] del Uruguay, donde se indican las materias curriculares que comprende cada curso a dictar. A partir de entonces, se convoca a elección de horas docentes, por Escuela, donde cada docente deberá elegir los grupos a los cuales dictará clases. Los docentes eligen sus horas mediante un sistema informático (Designaciones Docentes) el cual emite una Boleta de Designación que deberá ser presentada por el docente, en las Escuelas donde ha elegido impartir cursos. Posteriormente se completa un formulario de Declaración Jurada en cada una de las Escuelas donde están radicadas las horas elegidas por el docente.

El formulario de Declaración Jurada en cada una de las Escuelas se completa de forma manual. Es decir que, al tomar el cargo, cada docente llena en forma manual vía 5 copias una Declaración Jurada donde se estipula la situación del docente dentro de la UTU así como su situación a nivel de otras instituciones públicas y privadas. Dicha Declaración Jurada es enviada por correo convencional hacia la UTU Central.

Luego de la primera elección de horas se suceden situaciones de aumento o disminución de horas por diversas causas, lo que genera que en el correr del año se produzcan movimientos en las cargas horarias de los docentes. Esto provoca la liberación de horas que pasan a estar nuevamente disponibles para que puedan ser elegidas por otros docentes. Esto conlleva una gran problemática en cuanto al cobro de haberes correspondientes a horas dictadas, información que se toma de la Declaración Jurada docente.
Los cambios en la información referente a docentes asignados a cursos que se van produciendo en las sucesivas asignaciones y liberaciones de grupos por parte de los docentes producen errores de gran magnitud así como inconsistencia en los datos que se manejan.

Por otro lado, se están produciendo indeseados manejos internos, por parte del CETP, de la información que se desprende de las Declaraciones Juradas. Cada una de las copias de las Declaraciones Juradas es enviada a distintas oficinas dentro del CETP, donde se procesa dicha información dentro de sistemas informáticos diferentes. En el marco del proceso de integración que ya se está produciendo en el CETP, se busca integrar los sistemas informáticos de todas las oficinas hacia un esquema de bases de datos centralizados, donde los datos provenientes de las Declaraciones Juradas se depositen mediante un mecanismo automático de transferencia de datos, eliminando así su ingreso manual por cada una de las oficinas.

Motivados por la necesidad principal de recopilación de datos provenientes de las Escuelas y la necesidad de continuar con la integración de sistemas informáticos del CETP y la centralización de datos, el presente proyecto tiene como objetivo desarrollar un sistema para

[1] CETP = Consejo de Educación Técnico Profesional
[2] UTU = Universidad del Trabajo del Uruguay

el ingreso de las Declaraciones Juradas docentes en las Escuelas y su posterior envío de datos al sistema central.

Como parte del desarrollo se estudiarán diversas soluciones de conectividad entre las Escuelas y la UTU Central. La información será ingresada localmente en cada Escuela dentro de las bases de datos que maneja el programa de Bedelía Informatizada y luego será transferida a la **base de datos central** ubicada en el edificio Central de UTU. Esta información será tomada luego por los respectivos departamentos a los efectos de actualizar la situación actual de cada docente dentro de la Enseñanza, así como hacer efectivo el cobro de haberes correspondiente a la cantidad de horas asignadas al mismo. El sistema a desarrollar deberá formar parte del sistema de bedelía que ya se encuentra funcionando en las Escuelas (Bedelía Informatizada) pero no formará un punto más de su menú principal.

Actualmente, el envío de información que recoge el sistema de **Bedelía Informatizada**, desde las Escuelas hacia el Edificio Central, se realiza por medio de conexiones discadas, a través del programa PC-AnyWhere, que permite la transferencia de datos de forma remota. Hasta el momento, el uso de este programa ha traído aparejado serios problemas, en cuanto a que la conexión debe ser establecida desde el Edificio Central hacia las Escuelas y que no está produciendo los resultados esperados originalmente. Cabe acotar que las Escuelas no poseen conexión a Internet las 24 horas, por lo que no es posible que el ingreso de las Declaraciones Juradas se realice en forma online vía Web.

Otro aspecto no menos importante, es la necesidad del CETP de dejar accesible por Internet la información recopilada mediante las Declaraciones Juradas docentes, de forma tal que cada docente pueda acceder a sus datos privados cuando así lo requiera para realizar eventuales controles a dicha información. Interesa también publicar toda la información adicional referente a cursos, carreras, escalafones docentes, etc., que la institución desee publicar.

1.2 Objetivo y Alcance

El presente proyecto tiene como objetivo la realización de un producto que soluciona integralmente una problemática existente en UTU-CETP: la conectividad del Edificio Central con las Escuelas. Para ello se deberá analizar la posibilidad y forma de integrar los servicios de FTP, WEB y Mail a un modulo de procesamiento de datos.

El producto final debe permitir el ingreso de datos (Declaraciones Juradas) en las Escuelas, transferencia de datos desde las Escuelas hacia el Edificio Central de UTU y viceversa así como la consulta de datos “públicos” y “privados” a través de páginas Web, con control de acceso a nivel de usuario.

El proyecto debe establecer también la base física y lógica para futuras implementaciones por parte de la División Informática de UTU.

Alcance del Proyecto.

Se realizará un módulo de ingreso de Declaraciones Juradas que permita la transferencia de datos desde las Escuelas a UTU Central, que se integre a la ejecución del Sistema de Bedelías actualmente en producción en las Escuelas y que cargue los datos en la Base de Datos Centralizada en el Edificio Central de UTU. La puesta en producción de este módulo se

realizará solamente en algunas de las Escuelas de Montevideo, contemplando que, en un futuro, se incorporarán el resto de las Escuelas, incluidas las del Interior.

Se realizará un módulo de consulta de datos “públicos” y “privados” de la información existente en la Base de Datos Centralizada en UTU, a través de páginas WEB situadas en un servidor del Edificio Central de la misma. Se deberá analizar y desarrollar una solución de conectividad que garantice la seguridad de la información que podrá ser consultada a través de Internet.

2 Análisis de Requerimientos

El proyecto se divide en dos grandes módulos,

- Estudio e implementación del sistema de ingreso de Declaraciones Juradas
- Estudio e implementación del Sistema de Conectividad, que involucra dos grandes objetivos:
    - Transferencia de datos hacia el Edificio central de UTU, recogidos por las Declaraciones Juradas.
    - Publicación de información en Internet: información institucional pública y datos referente a la situación del docente en la institución (datos privados)

2.1 Sistema de Declaraciones Juradas

El sistema de Declaraciones Juradas presentará, como parte de su funcionalidad, el manejo los siguientes datos y acciones:

a) Alta, Baja y Modificación de Declaraciones Juradas

- Alta
    1. Alta de docentes
    2. Alta de grupos tomados por un docente
    3. Alta de acumulaciones dentro y fuera de ANEP
- Baja
    1. Baja de grupos tomados por docente
    2. Baja de acumulaciones dentro y fuera de ANEP

- Modificación
    1. Modificación de datos del docente
    2. Modificación de grupos tomados por el docente (liberar/tomar grupo)
    3. Modificación de acumulaciones dentro y fuera de ANEP.

Restricciones: (i)El resto de la información suministrada en la Declaración Jurada, como ser Egresos, Títulos Universitarios, Títulos CONAE, Grados y Efectividades del funcionario, solamente se desplegarán, no pudiendo ser dados de alta, baja o modificados por el docente. Estos datos serán suministrados por el CETP y depositados en los PCs locales de cada Escuela.
(ii) La Declaración Jurada debe mostrar la situación actual del docente dentro y fuera de ANEP.

b) Impresión de Declaración Jurada.

c) Envío de Datos hacia el Edificio Central UTU.
Los datos deberán ser cargados en la **Base de datos central** que se maneja en el Edificio Central de UTU.

d) Envío de Contingencia de datos (en caso de falla del punto c)

2.2 Sistema de Conectividad

Se pretenden desarrollar dos objetivos fundamentales en el área de conectividad: (i) un sistema de transferencia de datos referentes a las Declaraciones Juradas, desde las Escuelas hacia la base de datos única que se encuentra en el Edificio Central de UTU, con la consecuente estructura de envío y recepción de datos, usando como medio de transferencia de archivos alguna de las diferentes soluciones que surjan del estudio de conectividad y (ii) creación de un Sitio Web que ofrezca la información recopilada en el punto a) en Internet, así como información Institucional, cursos, carreras, etc.

Los objetivos de seguridad a nivel de red que se establecen son: (i) la red de UTU debe quedar aislada de Internet de forma de preservar su privacidad y seguridad de la información que allí se maneja asegurando su correcto funcionamiento, (ii) los usuarios poseerán correo electrónico (solamente los usuarios del edificio central y de las Escuelas) y (iii) navegación por Internet para usuarios con ciertos privilegios.

Para la etapa de desarrollo de la conectividad hacia Internet, UTU ofrece dos diferentes posibilidades mencionadas a continuación y ordenadas según su jerarquía de factibilidad. Ninguna de ellas se descarta hasta el momento de la puesta en implementación de los sistemas.

CONECTIVIDAD DE ANEP - CO.DI.CEN: ANEP cuenta con un sistema de Internet en funcionamiento, con los controles de seguridad requeridos para la realización de este proyecto. El Edificio Central de UTU, deberá entonces conectarse vía línea directa con la red de ANEP, formando parte de la misma, proyecto que ya está en estudio por parte de ambas instituciones. A partir de entonces, se contaría con acceso a Internet y posibilidades de uso de todo el equipamiento que para este uso ANEP dispone.

CONECTIVIDAD EN DIVISIÓN INFORMATICA
Existe la posibilidad de la contratación de una línea ADSL y la adquisición del hardware y software necesarios para que UTU pueda disponer de su propio sitio web, bajo el cual se ubicarían los módulos de consulta y transferencia de datos de Declaraciones Juradas.

El sistema de conectividad deberá resolver los siguientes requerimientos:

A) Implementación del Sitio Web en la División Informática de UTU ó conexión de la red UTU hacia el Sitio Web de ANEP-CODICEN, que permita la publicación en Internet de información general sobre la Institución donde cualquier usuario podrá acceder a esta información (datos públicos). Consulta de usuarios sobre datos privados donde el funcionario ingresará “nombre de usuario” y “clave” y podrá consultar los datos acerca de su situación dentro de la Enseñanza Técnico Profesional, tomada de sus Declaraciones Juradas.
Los módulos serán solamente de consulta de información, no permitiéndose en ningún caso modificaciones de datos.

B) Transferencia de Datos: Se determinará un sistema de transferencia de información desde y hacia las Escuelas, que podrá ser posteriormente migrado hacia otras aplicaciones de la División Informática. Inicialmente, este mecanismo deberá transferir la información de funcionarios de las Escuelas, recopilados mediante el sistema de Declaraciones Juradas. Se pretende en un futuro, la extensión de esta solución al Sistema de Bedelía Informatizada.

3 Diseño

Se construirán los siguientes sistemas:

a) Subsistema que permita el ingreso de las Declaraciones Juradas, que se integrará al sistema de Bedelía Informatizada con que ya cuentan las Escuelas.
   Finalizado el proceso de ingreso de todas las Declaraciones Juradas correspondientes, el usuario deberá iniciar la operación de envío de información hacia el Edificio Central.
b) Sistema Web de consulta de datos referentes a la información recibida de las Escuelas en lo que a Declaraciones Juradas respecta. Tanto las escuelas como cualquier docente, vía Internet, tendrá la posibilidad de chequear la información correspondiente, dependiendo del tipo de datos que desee consultar: públicos o privados.
c) Se deberá implementar el sistema de conectividad para los diseños informáticos mencionados en los puntos a y b.

3.1 Diseño Sistema Declaraciones Juradas

3.1.1 Modelo Entidad Relación – Bedelía Informatizada Existente.

El sistema de Bedelía Informatizada que se encuentra en funcionamiento en las Escuelas cuenta con el diseño de estructura de datos que se presenta a continuación.

Solamente se reflejan en este modelo las estructuras que se relacionan con el ingreso de las Declaraciones Juradas.

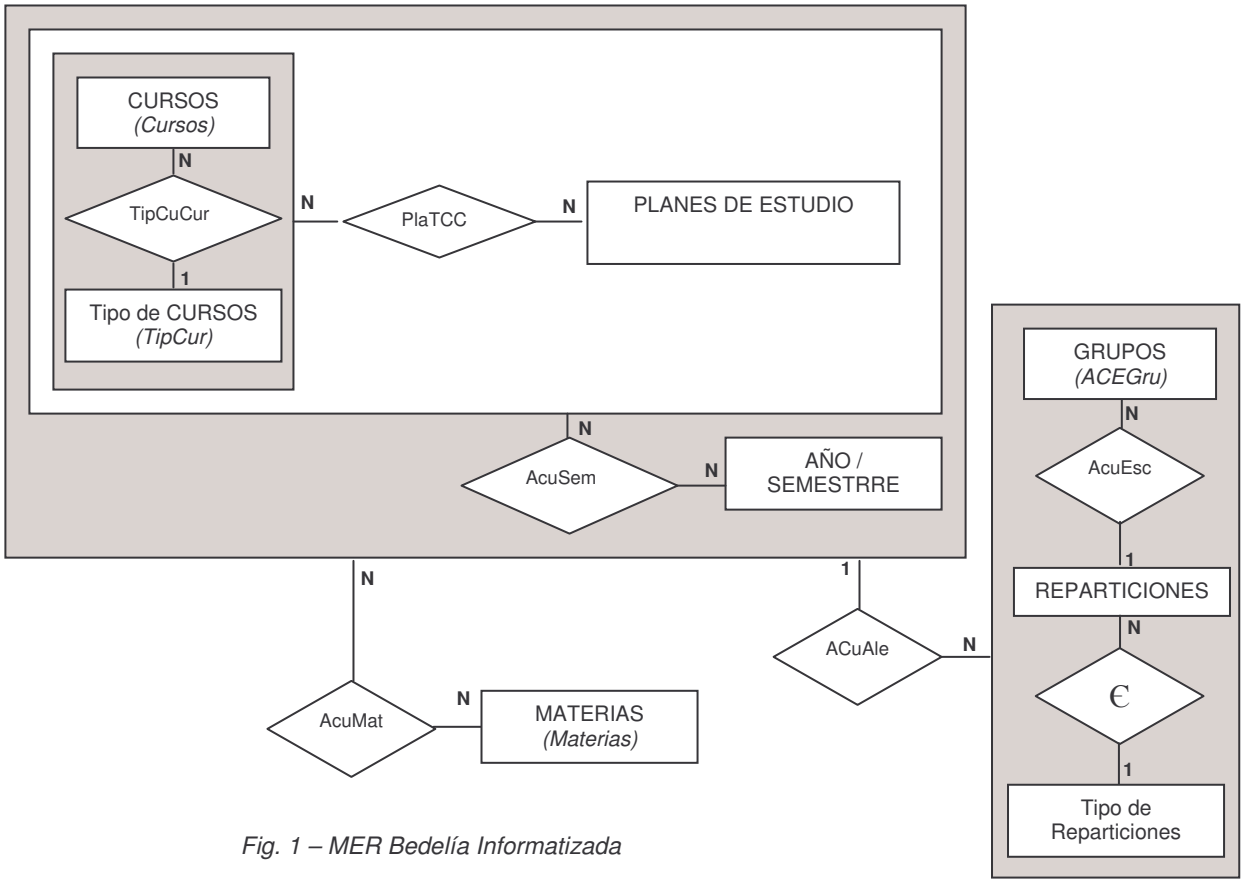


Fig. 1 – MER Bedelía Informatizada

Identificación de objetos
Se identifican los siguientes objetos:

Cursos
Tipo de Cursos
Planes de Estudio
Materia
Años / Semestres
Grupos
Reparticiones
Tipo de Reparticiones

Identificación de Relaciones
Se identificaron las siguientes relaciones:

TipCuCur:	Un curso tiene un tipo determinado
PlatCC:	Un plan de estudio tiene cursos asignados de ciertos tipos.
AcuSem:	Año y semestre en que se dictan los cursos de un determinado plan de estudio.
AcuEsc:	Un grupo pertenece a una repartición (escuela).
AcuMat:	Materias que se encuentran asociadas a un curso.
AcuAle:	Cursos de un determinado plan de estudios asociados a grupos de una determinada repartición.

Identificación de Atributos

GRUPOS

GRUPO	(Código de Grupo)
DESCRIPCION	(Descripción de Grupo)
AÑO LECTIVO	(Año Lectivo)
SEMESTRE	(Semestre Lectivo)
PLAN	(Código de Plan)
TIPO CURSO	(Código de Tipo de Curso)
CURSO	(Código de Curso)
ANIO CURSO	(Año dentro del Curso)
SEMESTRE CURSO	(Semestre Dentro del Curso)
REPARTICION	(Código de Repartición)
DESCRIPCION GRUPO	(Descripción de Grupo para Escuela)
TURNO	(Código de Turno)
DIAS CLASES	(Días clases técnicas)
USUARIO	(Nombre de Usuario que actualiza datos)
ACTUALIZACION	(Fecha de última actualización)
HORA	(Hora de última actualización)

CURSOS

CODIGO	(Código de Curso)
DESCRIPCION	(Descripción del Curso)
DESCR. ABREV.	(Descripción Abreviada del Curso)

TIPOS DE CURSOS

CODIGO	(Código de Tipo de Curso)
DESCRIPCION	(Descripción de Tipo de Curso)
DESCRIP. ABREV.	(Descripción Abreviada del Tipo de Curso)

PLANES DE ESTUDIO

CODIGO	(Código de Plan)
DESCRIPCION	(Descripción del Plan)
RESOLUCION	(Fecha de Resolución)
ACTA	(Acta de Resolución)
NOTA	(Nota de Resolución)

MATERIAS

CODIGO	(Código de Materias)
DESCRIPCIÓN	(Descripción de Materia)
DESC_ABREVIADA	(Descripción Abreviada)

REPARTICIONES

CODIGO	(Código de Repartición)
NOMBRE	(Nombre de Repartición)
NOMBRE ABREV.	(Nombre Común Abreviado)
HACIENDA	(Código de Hacienda)
TIPO DE REPARTICION	(Código Tipo de Repartición)
NRO. INVENTARIO	(Ultimo numero de Inventario en la Repartición)
DEPARTAMENTO	(Código de Departamento)
RELACION JURIDICA	(Relación Jurídica)
CALLE	(Calle de la Repartición)
NUMERO	(Numero de calle de la Repartición)
TELEFONO	(Teléfono)
USUARIO	(Login de Usuario que elimina/modifica)
FECHA	(Fecha en que se elimina/modifica)
HORA	(Hora en que se elimina/modifica)

TIPO DE REPARTICION

CODIGO	(Código del Tipo de Repartición)
NOMBRE	(Nombre del Tipo de Repartición)

3.1.2 Modelo Entidad Relación – Sistema Declaraciones Juradas.

Se busca integrar el formulario de Declaraciones Juradas que guardará los datos del estado de situación del funcionario con respecto a UTU y otras dependencias estatales, con la información referente a los cursos y materias que el docente dicta.
Para ello se desarrollará un sistema de ingreso de Declaraciones Juradas, que se integre al sistema informático de Bedelía, mencionado en el apartado anterior, y que actualmente se encuentra funcionando en las Escuelas de todo el país.

Se presenta a continuación, los datos que recopilan las Declaraciones Juradas:

A. DATOS GENERALES: Se ingresará el nombre de la Escuela donde se completa la Declaración Jurada, los datos personales del docente, ingreso a la Administración pública, ingreso a la docencia e ingreso a la Universidad del Trabajo del Uruguay.

B. SITUACION ANTERIOR EN LA REPARTICIÓN: Interesa conocer el total de horas básicas y escalafonadas en esta repartición, que el docente poseía el año anterior.

B. TITULOS C.O.N.A.E: Interesa conocer si el docente posee títulos CONAE y en caso afirmativo, la fecha en que se emitió.

C. TITULOS PROFESIONALES UNIVERSITARIOS: Interesa conocer si el docente posee títulos profesionales universitarios y en caso afirmativo, la fecha en que se emitió.

D. SITUACION ACTUAL EN LA REPARTICIÓN: Se despliegan los grupos que el docente tiene asignado en el corriente año lectivo, dentro de la Escuela donde se completa el formulario de Declaración Jurada. Se muestra la información referente al grupo como ser asignatura a dictar, curso, área, tipo de cargo docente, cantidad de horas a dictar, fecha de posesión del grupo y total de horas semanales (sumando todos los grupos que posee a su cargo en esta repartición).
En el caso de que el cargo sea una suplencia, importa conocer los datos del titular: Cédula de Identidad y el motivo de la ausencia.

E. CARGOS DENTRO DE ANEP: Si el docente se encuentra dictando clases dentro de otra institución dentro de ANEP interesa conocer el nombre de la Repartición, la asignatura, la fecha de posesión del cargo y la cantidad de horas asignadas.

F. OTROS CARGOS PUBLICOS FUERA DE A.N.E.P.: Si el docente se encuentra desempeñando tareas en otros cargos públicos fuera de ANEP, interesa conocer el nombre de la empresa, el cargo que desempeña, la fecha de posesión del cargo y la cantidad de horas asignadas.

G. BAJA DE CARGOS: En caso de baja de cargos o liberación de horas docentes, se deberá ingresar la fecha e información referente al motivo por el cual se produce el cese.

Un dato importante a conocer, proveniente del análisis de requerimientos, es la necesidad de completar una Declaración Jurada ante cualquier movimiento de datos referentes al funcionario. En lo que a liberación de grupos respecta, al completar la Declaración Jurada se debe visualizar la situación actual que presenta el docente en la Escuela al momento de completar dicho Formulario y los grupos que se liberan desaparecen de la Declaración Jurada. Por ejemplo, si un docente toma 3 grupos éstos aparecen en su Declaración Jurada. Si posteriormente decide renunciar a uno de ellos, se deberá realizar una nueva Declaración Jurada donde se visualizarán los grupos que posee al momento de la Declaración Jurada, es decir 2 grupos.

En la figura 2 se presenta el MER correspondiente al sistema de Declaraciones Juradas a implementar.

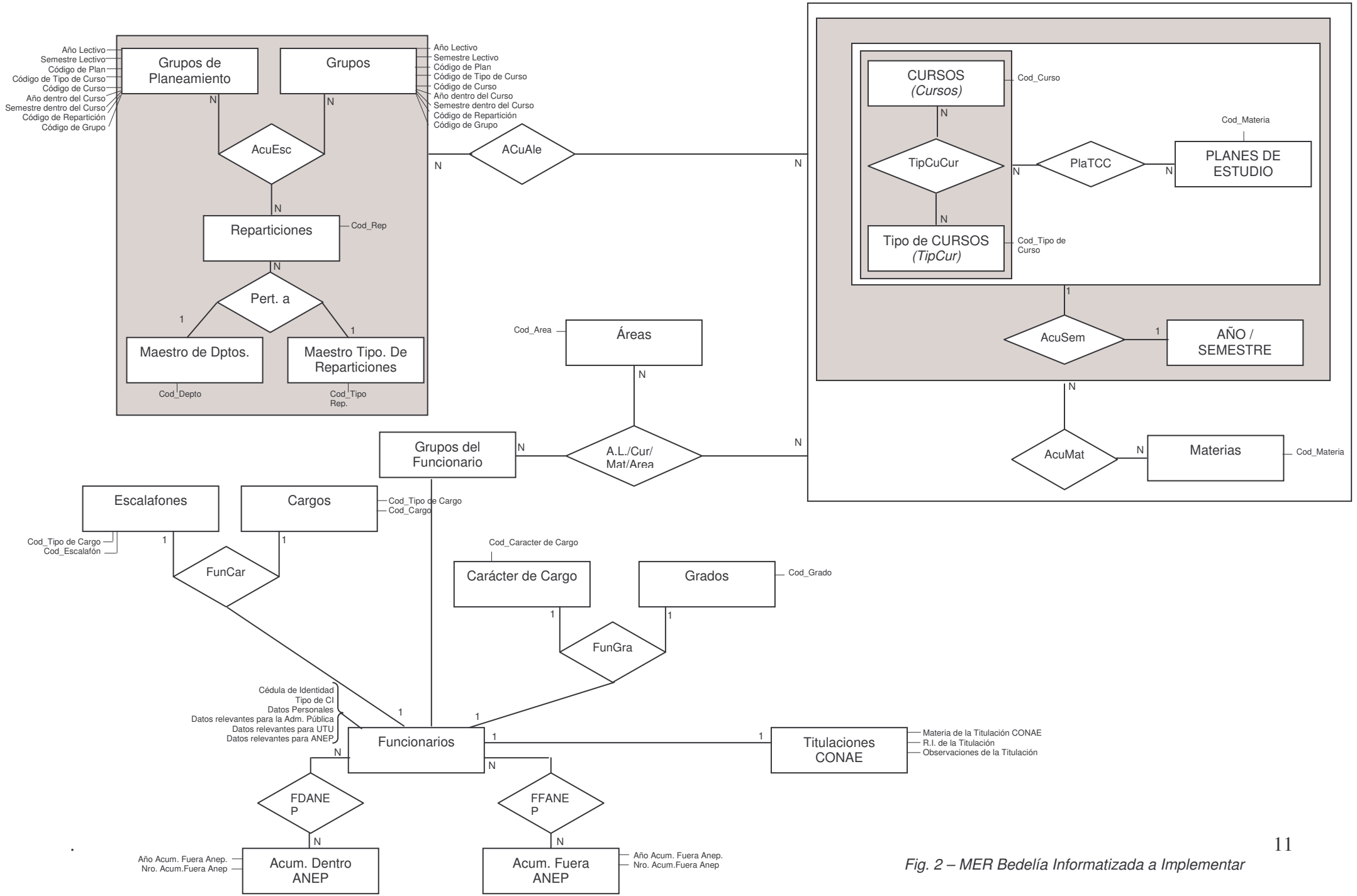


Fig. 2 – MER Bedelía Informatizada a Implementar

Identificación de objetos
Se identifican los siguientes objetos:

Grupos
Grupos de Planeamiento.
Reparticiones
Maestro de Tipos de Reparticiones
Maestro de Departamentos
Cursos
Tipo de Cursos
Planes de Estudios
Áreas
Materias
Funcionarios
Escalafones
Cargos
Carácter del Cargo
Grados
Acumulación dentro de ANEP
Acumulación fuera de ANEP
Titulaciones CONAE
Grupos asignados a funcionarios: grupos que el docente toma a su cargo.

Identificación de Relaciones
Se identificaron las siguientes relaciones:

AcuEsc	Cursos de una determinada escuela según Planeamiento.
AcuAle	Año – Semestre – Curso – Año Lectivo
TipCuCur	Cursos – Tipos de Cursos
PlaTCC	Planes – Tipos de Cursos – Cursos
AcuMat	Áreas – Año – Materia
AcuSem	Cursos– Años – Semestres
ACMAre	Año Lectivo – Curso – Materia – Área
FunGra	Funcionarios – Grados – Carácter de Cargo
FunCar	Funcionarios – Cargos
FDANEP	Acumulación dentro de ANEP
FFANEP	Acumulación fuera de ANEP
ACMAre	Año Lectivo – Curso – Materia - Área

Identificación de Atributos
En el apéndice B se explica en detalle la información referente a tablas y atributos correspondientes.

RESTRICCIONES ASUMIDAS

1) Las declaraciones Juradas se mantendrán año a año en el sistema y no se eliminarán por ningún concepto del sistema de Bedelía Informatizada.
2) Cuando el funcionario docente asume su cargo debe completar una Declaración Jurada con su situación actual dentro de la repartición.
   Cuando por algún motivo el funcionario renuncia a sus grupos, debe llenarse otra declaración jurada donde aparecen solamente los grupos que actualmente mantiene,

desapareciendo de la declaración jurada aquellos a los cuales renuncia. Es en este caso cuando se completan los campos que corresponden a la baja de horas.
En resumen, ya sea en la toma de posesión o en la de liberación de grupos, se debe completar una Declaración Jurada donde se refleje la situación de grupos que el funcionario posee, al día de la fecha de completada la Declaración Jurada.

3) El cargo del funcionario se obtiene de la tabla **Cargos**
4) El grado del funcionario se obtiene de la tabla **Grados**.
5) Para cada materia, un docente tiene una sola titulación de CONAE.
6) La tabla Grupos de Planeamiento es transferida desde el Edificio Central de UTU hacia las Escuelas y contiene los datos de los grupos que se abrirán en el corriente año lectivo. Estos datos son librados por la oficina de Planeamiento.
7) Las titulaciones de CONAE se deben referir a la tabla MATERIAS
8) Los Grupos del funcionario deben ser grupos correspondientes a la planilla de grupos enviado por la oficina de Planeamiento.
9) Los códigos de área requeridos en el sistema son tomados de la tabla **Áreas**.
10) Año lectivo, curso y materia determinan un Área.

3.1.3 Especificación de Procesos

Se presentará a continuación, en lenguaje de alto nivel, la lógica del funcionamiento del sistema de Declaraciones Juradas presentando el menú principal y luego los módulos que de allí se desprenden: Alta, Baja y Modificación de Funcionarios, de Grupos y de Acumulaciones Dentro y Fuera de ANEP así como Transferencia de datos desde las Escuelas hacia el Edificio Central de UTU.

Menú Principal:

```
Loop
    Ingresar usuario
    Si es un usuario válido para operar el sistema
      - ABM de Declaraciones Juradas
        -Ingresar código de funcionario
        -Si el funcionario existe entonces
                -desplegar datos del funcionario
        -sino
                -habilitar el alta de datos del funcionario
        -Si se ingresó código de funcionario
                -habilitar el ingreso, baja o modificación de:
                        -grupos de funcionario
                        -acumulaciones dentro ANEP
                        -acumulaciones fuera de ANEP
                        -impresión de la Declaración Jurada del docente
        -sino
                -Msg (ingrese código de funcionario)
      - End ABM de Declaraciones Juradas

      - Envío de datos al CETP.
SINO
        Msg (Ingrese nombre de usuario y contraseña)
```

EndLoop
End Menú Principal.

Alta, Baja y Modificación de Grupos del funcionario

-Nuevo Grupo: Alta de Grupo para el docente
-Borrar Grupo: Se permite borrar un grupo en caso de error de digitación
-Liberar un Grupo: Al liberar un grupo se le asigna la fecha y motivo por el cual se libera. No se borra el grupo del sistema.
-Tomar un Grupo: Permite que el curso sea retomado por un docente.

Nota: se deberá llenar una Declaración Jurada para el docente ante cualquier movimiento de la situación actual dentro de la repartición, es decir una Declaración Jurada tanto ante la toma de posesión de un grupo como ante la baja del mismo. La última Declaración Jurada siempre debe reflejar la situación actual del funcionario dentro de la repartición.

Alta, Baja y Modificación de Acumulaciones dentro de ANEP

-Alta de acumulación dentro de ANEP.
-Baja de acumulación dentro de ANEP
-Modificación de acumulación dentro de ANEP

Alta, Baja y Modificación de acumulaciones fuera de ANEP

- Alta de acumulación fuera de ANEP.
- Baja de acumulación fuera de ANEP
- Modificación de acumulación fuera de ANEP

Impresión de Declaración Jurada del Docente

-Solicitar número de copias a imprimir (por defecto 5)
-Mientras el total de copias < = nro. de copias solicitadas
  -Imprimir datos del funcionario
  -Imprimir grupos del docente
  -Imprimir acumulaciones dentro de ANEP
  -Imprimir acumulaciones fuera de ANEP.
-Fin Mientras

3.2 Propuestas de Diseño de Conectividad

El presente estudio de las diferentes propuestas de conectividad se basó en la información recopilada en los apéndices C, D y E.

Buscando resolver e integrar dos problemas importantes como ser la presencia de UTU en Internet y la transferencia de datos desde las Escuelas hacia el CETP, se plantea como solución fundamental la implementación de un Sitio Web, el cual se basará en un sistema de Firewall a nivel de aplicación.

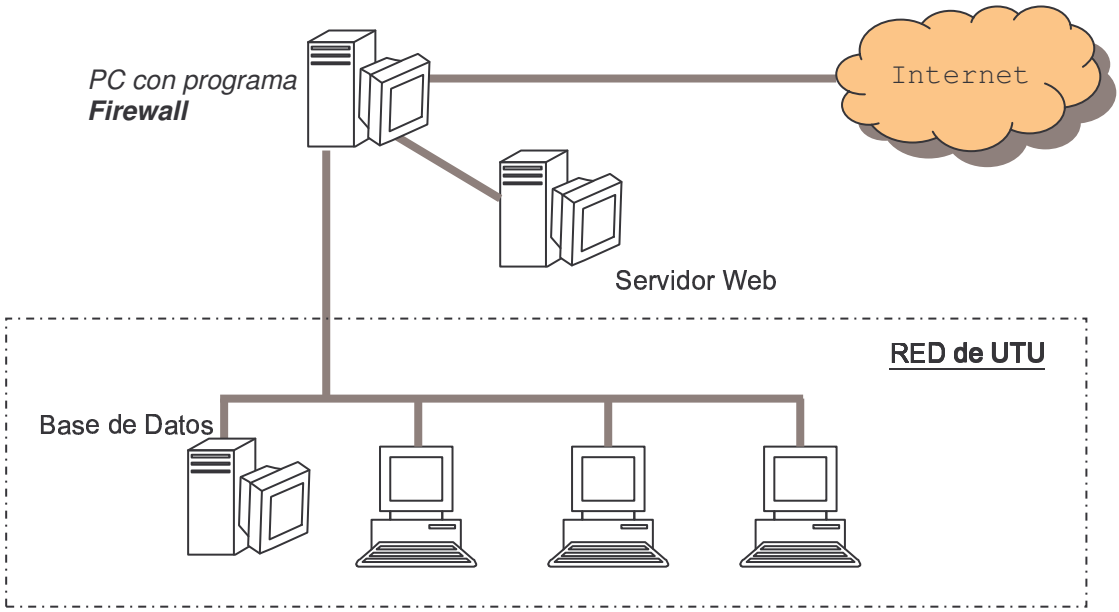


Fig. 3 – Diseño Conectividad General

En la figura 3 se muestra el esquema general de conexión, donde se puede observar que la red de UTU será aislada de Internet mediante un Firewall implementado por hardware o por software. La base de datos del sistema quedará aislada dentro de la red de UTU, estando el Servidor Web fuera de dicha red directamente conectado al Firewall, admitiendo accesos desde y hacia Internet a través de él. El Servidor Web contendrá la información necesaria para la publicación en la Web y en él las Escuelas depositarán la información referente a la transferencia de datos.

El Firewall será el sistema básico de seguridad que se basa en la instalación de una "barrera" entre la red de UTU y la red Internet. El tráfico entre Internet y la red será autorizado o denegado por el Firewall, siguiendo las instrucciones de configuración que se le designen (Internet → PC's ó PC's → Internet)

Se pretende implementar las siguientes reglas de seguridad:

(i) FTP entrante y FTP saliente. Este servicio permitiría la transferencia de datos entre UTU y las Escuelas mediante Internet, ya sea que las Escuelas depositen datos en el servidor (datos obtenidos mediante el sistema de Declaraciones Juradas u otros sistemas que se desee) como que las Escuelas tomen datos del mismo (por ejemplo, cursos que se dictarán en el corriente año lectivo,

requeridos por el sistema de Declaraciones Juradas, y que son liberados por el Programa de Planeamiento).

(ii) acceso al Sitio Web del CETP con restricciones a nivel de acceso de usuarios. Se debe implementar la posibilidad de que se brinde información pública (sin acceso de usuario) de la Institución así como información privada mediante el inicio de una sesión de usuario en el Sitio Web. Asimismo, se aconseja que la transferencia de datos se realice previo inicio de una sesión en el servicio FTP

(iii) control de acceso a Internet a usuarios de la red de UTU debidamente autorizados (no todos los usuarios de la red dispondrán salida a Internet).

El servicio FTP permite la transferencia de archivos desde y hacia Internet. A través de este servicio, el servidor de FTP debe ofrecer carpetas dentro de su sistema de archivos donde las Escuelas, previa validación de usuario puedan depositar los archivos generados por el Sistema de Declaraciones Juradas, por el Sistema de Bedelía Informatizada y en un futuro, datos provenientes de otros sistemas que se implementen. Una vez que los datos hayan sido transferidos, un programa (por ejemplo un programa de barrido) deberá recoger los datos e insertarlos en la Base de Datos Central de UTU.

Ante posibles ataques desde Internet hacia la red de UTU, el Servidor Web se encontrará aislado de la red, en un dominio aparte, pudiendo ser accedido desde la red de UTU. Los accesos por parte de Internet serán entonces realizados hacia dicho servidor Web, no permitiéndose accesos hacia la red de UTU. Se debe crear una zona desmilitarizada (DMZ-Apéndice C) que permita asegurar la confiabilidad y seguridad de la red Institucional de UTU, estando aquí el Web Server y otros servidores que se requieran (por ejemplo el Servidor de correo). Existen varias posibilidades de elección de Firewall que se implementan tanto por hardware como por software. Por un tema de costos, y dado el potencial uso e implementación de seguridad así como de mantenimiento que se desarrollado la tecnología en los últimos tiempos, se sugiere la implementación de un Firewall a través de software, que viene incluido con el sistema operativo Linux.

SOLUCIONES DE CONECTIVIDAD

A continuación se describen las distintas soluciones de conectividad que fueron analizadas.

Como primera alternativa, el CETP ofrece la posibilidad de salida hacia Internet implementando la conectividad mediante el enlace de la red de UTU con la red de ANEP, quienes prometen el uso por parte del CETP de su Sitio Web así como de servicios que ya poseen implementados y que se encuentran en correcto funcionamiento.

Como segunda alternativa, se estudia la posibilidad de implementar el Sitio Web sin recurrir a ANEP, es decir desarrollando el Sitio Web en el Edificio Central de UTU. Evidentemente es una solución más costosa y con mayores inconvenientes en cuanto a mantenimiento y administración de dicho Sitio.

Luego, se describen otras soluciones de conectividad en cuanto a transferencia de datos se refiere, creando una solución para el envío de información desde las Escuelas hacia UTU y viceversa. Se descarta totalmente la presencia de UTU en Internet así como el sistema de consultas de datos públicos y privados vía online.

Finalmente se plantea una solución "ideal" con vistas a futuro la que ofrecería una mayor cantidad de prestaciones posibles en cuanto a conectividad se refiere, pero con poca viabilidad a corto plazo.

1) CONECTIVIDAD DE ANEP - CO.DI.CEN.

Como primera solución, se presenta el acceso al Sitio Web de ANEP-CODICEN, el cual se encuentra actualmente en funcionamiento con las funcionalidades de HTTP y FTP que se requieren en este proyecto.

Hasta el momento, no fue posible conocer el tipo de conexión que se requeriría para conectar ambas redes. Tras reuniones sucesivas entre UTU y la división Informática de ANEP, no se ha determinado una resolución al respecto, así como no se conoce en detalle la información necesaria. Por lo tanto, hubo que realizar un estudio detallado de las posibilidades dependiendo del tipo de conexión (Frame Relay o Data Express).

En ambos casos el Sitio Web sería íntegramente gerenciado por ANEP-CODICEN, disponiendo de lugares físicos donde depositar los datos para la transferencia FTP, así como para la publicación de información en el Sitio Web de ANEP. Se debe destacar que la red de UTU no pasará a formar parte de la red de ANEP, sino que solamente utilizará el servidor Web que ANEP posee. ANEP, que ofrece el servidor Web, publicará las páginas web que UTU le entregue y recogerá los archivos resultantes de la transferencia de datos desde las Escuelas, para luego ser retirados por el responsable de la administración de la información e insertados en la base de datos central de UTU. Hasta el momento se desconoce en su totalidad el sistema Web que ofrece ANEP en cuanto a su implementación y funcionamiento lo que posiblemente requiera un refinamiento futuro de esta solución.

Como se observará en ambos esquemas de conectividad, el servidor de Bases de Datos de UTU, que se encuentra dentro la red donde se ubica la Base de Datos Única del Sistema, no será accedido por ANEP en ningún momento, por lo tanto, tampoco será accedido desde Internet.

a. Conexión vía Frame Relay

Cabe la posibilidad de que la red de ANEP concentre varios puntos remotos en un punto principal a través de un único enlace, disminuyendo así el costo en equipos de comunicaciones. En este caso, estamos en presencia de una conexión Frame Relay.

El sistema de interconexión entre la red de UTU y la red de ANEP requiere en este caso, la instalación de un router por parte de UTU, la contratación de una línea FrameRelay y la instalación y configuración de un servidor Firewall que aísle ambas redes, brindando protección y seguridad. Antel[3] ofrece para líneas Frame Relay velocidades desde 16 Kbps en adelante.

[3] Proveedor de servicios consultado

El esquema de conectividad sería el siguiente:

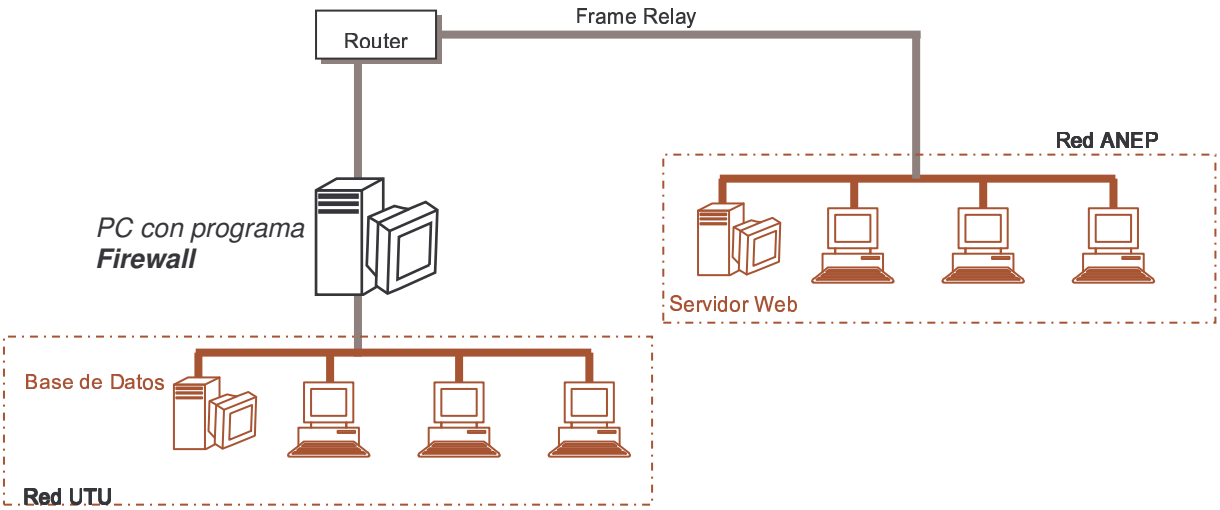


Fig. 5 – Conexión FrameRelay

b. Conexión vía línea Data Express

En el caso de que la conexión entre ANEP y UTU sea de extremo a extremo, se requiere el uso de una línea directa digital, brindada por el servicio Data Express. Se requerirá en la implementación de esta conexión dos routers: uno del lato de la red de UTU y otro del lado de la red de ANEP así como la contratación de una línea Data Express y la implementación de un sistema Firewall que aísle ambas redes brindando protección y seguridad. Antel ofrece para líneas Data Express las siguientes velocidades: 10 Mbps interfaz ethernet, 100 Mbps interfaz fast-ethernet y 155 Mbps ATM interfaz STM1 – óptica.

El esquema de conectividad que se plantea es el siguiente:

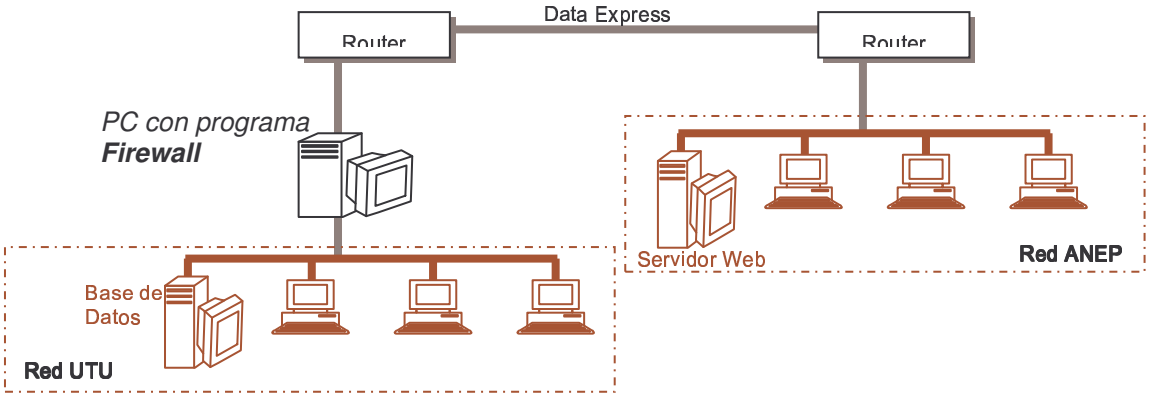


Fig. 4 – Conexión DataExpress

2) CONECTIVIDAD EN DIVISIÓN INFORMATICA

A continuación se presentan las soluciones de conectividad que brindan la presencia corporativa de UTU en Internet, permitiendo desarrollar e implementar un Sitio Web Institucional, enteramente administrado por personal de UTU, con la subsiguiente plataforma

de transferencia de información desde y hacia las Escuelas. Se podrán tomar en este caso, soluciones de futuro que ofrezcan más potencialidad al sistema de conectividad que se presenta en este estudio, brindando nuevos servicios que así se requieran.

Se presentarán a continuación las diferentes soluciones que se pueden aplicar. Todos los sistemas mencionados y que se estudiarán a continuación, aplicados a la realidad que se intenta resolver en UTU, se basan en el esquema de conectividad general que se muestra en la figura 6.

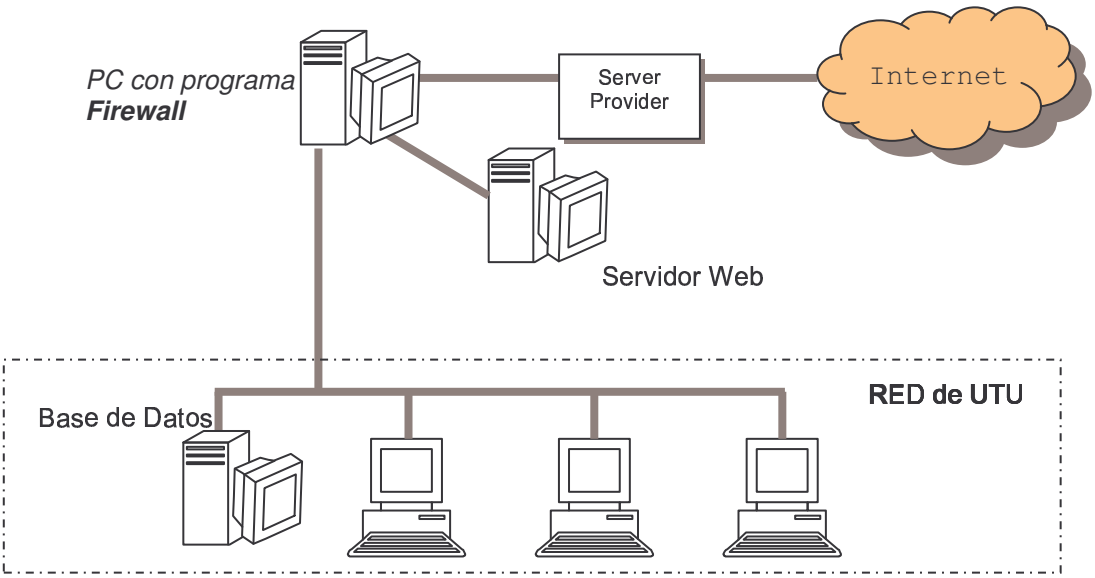


Fig. 6 – Acceso Dedicado / Internet

Como se puede observar en este dibujo (y ha sido mencionado a través de todo este estudio de conectividad) se deberá aislar la red de UTU mediante un Firewall, ubicando el Servidor de Páginas Web en un dominio aislado con un sistema de seguridad bien establecido. El servicio de Firewall puede ser brindado por una solución de hardware o de software. En el mercado existen diferentes opciones a nivel de hardware siendo su costo elevado. Por otro lado existe una solución a nivel de software que está siendo utilizada cada vez más en los últimos tiempos por muchas empresas con mayor aceptación debido a sus grandes posibilidades en cuanto a seguridad, administración y bajos costos. Estamos hablando del servicio Firewall que ofrece el sistema operativo Linux. Para este equipo serán necesarias tres tarjetas de red, una para la línea de conectividad hacia Internet, otra para conectarse al Sito Web y la otra para conectarse a la red de UTU. Para este equipo se requerirá la contratación de una dirección IP estática.

Para el Servidor de páginas Web se puede elegir el sistema operativo y servidor de páginas web que se desee, eligiendo soluciones que van desde Linux (de bajo costo con mejoras en Internet accesibles online) hasta soluciones Microsoft. El dominio ya se encuentra contratado por ANEP (www.utu.edu.uy), pero está siendo él administrado.
Este equipo deberá poseer una tarjeta de red y se deberán correr los servicios Web y FTP como mínimo. Además se requerirá la utilización de otra IP estática y por supuesto, la contratación de una línea que ofrezca la conectividad hacia Internet, provista por algún Proveedor de Servicios.

Para la transferencia de datos se deberá instalar el servicio FTP entrante (transferencia de datos desde las Escuelas a UTU) y saliente (transferencia de datos desde UTU hacia las

Escuelas), con control de usuario en el inicio de la conexión y su posterior desconexión del sistema. Para ofrecer más seguridad sobre la transferencia de datos, se podría implementar el servicio FTP corriendo sobre VPN (Virtual Private Networks), a través de Internet. Este servicio establece la conexión del cliente (Escuela) hacia el servidor de VPN, usando como canal de comunicación a la red Internet . Se crea un túnel de uso exclusivo de la Escuela y del Servidor, estando los datos encriptados según protocolos especiales, que serán transferidos luego por Internet, a través del protocolo TCP/IP. Este mecanismo sería muy útil en planificaciones futuras, dado que permitiría el acceso a los sistemas de UTU en forma online las 24 horas del día, hacia las Escuelas.

En la figura 7[4] se observa la existencia de dos posibles conexiones: una posibilidad es la conexión dedicada hacia Internet con todas las prestaciones que ello implica, la otra es la conexión dedicada con UruguayNet y Redes Regionales facilitando un rápido acceso a la información. Otra posible solución es la conexión mediante el acceso a Internet mediante el servicio *Internet Class,* con otras prestaciones que se mencionan más adelante.

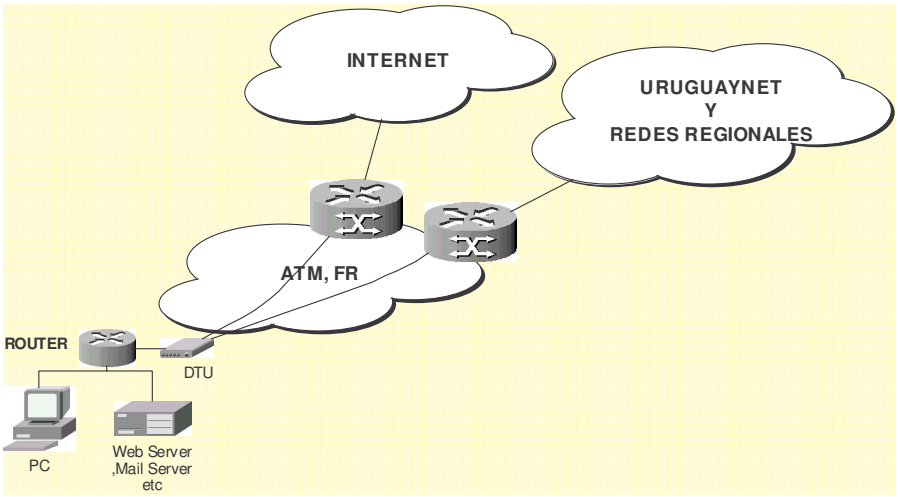


Fig. 7 – Servicio Dedicado a Internet

Servicio Dedicado a Internet.

Es un servicio digital en su totalidad en el cual se ofrece conectividad total y permanente con Internet, local, regional y global. Se garantiza el ancho de banda hasta el nodo de Internet en estados unidos.

El proveedor de servicios brinda un dominio y las direcciones IP públicas fijas necesarias para la red del cliente. Incluye Unidad de Terminación de datos del enlace digital, mantenimiento del router suministrado y supervisión centralizada de la red en forma permanente.

Este servicio ofrece velocidades de 64 kbps, 128 kbps y 256 kbps. El cliente (Escuelas) deberá realizar el acceso discado a Internet discando al 09091234 en línea telefónica normal ó al 09091264 a través de ISDN, sin usuario ni contraseña.

[4] Figura tomada de www.anteldata.com.uy

Línea Dedicada a URUGUAYNET

Este es un servicio de acceso dedicado a UruguayNet, basado en líneas directas digitales, que ofrece conectividad total y permanente con la red UruguayNet (Uruguay y países limítrofes).

El servicio incluye:

- Administración y mantenimiento del router suministrado en UTU
- Direcciones IP necesarias y dominio.
- Velocidades de 64, 128 y 256 Kbps.

A nivel del cliente (Escuelas) se debe considerar lo siguiente:

- El acceso se realiza a través del número telefónico 11133 ó por el 11164 (a través de RDSI) con usuario@adinet.
- Se requiere de un software que le permita establecer una conexión (discado) y establecer el protocolo PPP (Point to Point Protocol)

Servicio INTERNET CLASS

Es un servicio digital y bidireccional de alta velocidad, que comparte con otros servicios de su tipo el canal internacional sobre fibra óptica a la red Internet. Ofrece dominio y 5 direcciones IP fijas. Posee supervisión centralizada para realizar el mantenimiento, operación y gestión de la red y de los equipos en forma permanente. Exige interfase de red Ethernet (10 base T) del lado del cliente

El cliente (Escuelas) deberá realizar el acceso discado a Internet discando al 09091234 en línea telefónica normal ó al 09091264 a través de ISDN, sin usuario ni contraseña.

3) – OTRAS SOLUCIONES PARA TRANSFERENCIA DE DATOS

Se presenta a continuación un análisis de las diferentes formas de transferencia de datos desde UTU hacia las Escuelas y viceversa. Se estudiarán las soluciones de transferencia de datos a través de: RAS (Remote Access System), discado telefónico utilizando un rack de módems, correo electrónico y por último disquetes. Cabe recordar que estas soluciones ofrecen solamente un mecanismo de transferencia de datos, no así la implementación de un Sito Web en Internet.

Conexión vía RAS

La conexión vía RAS permitirá que el cliente, discando a un número telefónico de UTU Central, vía login, se conecte a la red Institucional de UTU, pasando a formar parte de la red interna. La transferencia de datos es simplemente una transferencia de máquina a máquina de la red, con un simple copiado de archivos entre carpetas.

A partir de la versión de Microsoft Windows 2000, es posible que el servidor realice la llamada al cliente, evitando los costos que se originarían en las llamadas de las Escuelas hacia Montevideo. Todo el costo estaría asumido en el Edificio Central de UTU, tal cual se viene desarrollando hasta el momento.

Se requiere:

- 1 PC con sistema operativo Windows 2000 (o superior) o sistema operativo Linux. A partir de Windows 2000, el servicio RAS permite que el servidor disque hacia los cliente. Linux ofrece la misma posibilidad, a través de Red Hat 6.x [12]
- 1 línea telefónica dedicada las 24 horas del día.

El equipo que oficiaría de servidor RAS, debería ubicarse en el Edificio Central de UTU. Esta solución trae aparejado el problema de que se debería instalar Escuela por Escuela el servicio cliente necesario para habilitar esta funcionalidad.
Además, este modelo sólo acepta que el servidor se conecte con una Escuela por vez. Si las Escuelas del Interior del país desean transferir los datos hacia el Edificio Central de UTU, deberán realizar las llamadas telefónicas hacia Montevideo, lo cual tiene un costo asociado elevado. La solución a este inconveniente sería que se discara desde UTU hacia las Escuelas, costo que ya se viene manejando en la actualidad con el uso del programa PCAnywhere.

RACK DE MODEMS

Se requerirá de la instalación de un rack de módems, los cuales podrán recibir llamadas de las Escuelas, o en su defecto, se podrá llamar a las mismas.

Para la implementación de esta solución se requiere:

- Servicio BL que ofrece ANTEL como colectivo de llamadas (entrantes/salientes en todas sus combinaciones)
- Router que maneja módems analógicos (ej. PM2 Postmaster 2 de Lucent) ó equipo que maneja módems digitales (ej. PM3 con módems de 56K, incluidos en el router).

Esta solución acepta la conexión de más de un cliente por vez, estando acotada por la cantidad de módems y la línea que brinda ANTEL.

Al igual que en el caso anterior, habría un costo elevado relativo a las llamadas de las Escuelas del Interior hacia el Edificio Central de UTU. Esto también se resolvería discando desde UTU hacia las Escuelas, mediante el uso del PCAnyWhere.

TRANSFERENCIA DE DATOS VIA EMAIL

Otra solución posible, que requeriría el mínimo costo asociado, es el envío de los datos vía Email. Todas las escuelas ya poseen una dirección de correo electrónico creada en el servidor de correo de ANEP, habilitado las 24 horas.

Se requeriría, en éste caso, de un chequeo previo de que las máquinas de las Escuelas posean un módem instalado y configurado así como el acceso a una línea telefónica que permita el ingreso a su buzón de correo en Internet.

Cabe observar, que el servicio de email de ANEP no es demasiado confiable, debido a caídas demasiado frecuentes de dicho sistema de correo. En caso de implementar un servicio de correo por parte de UTU, se podría entonces considerarlo como solución. Genexus posee herramientas de gerenciamiento de información enviada por mail electrónico, para su posterior utilización, lo cual permitiría integrar al sistema informático en actual desarrollo, un mecanismo de transferencia de datos vía email, para su posterior almacenamiento en la Base de datos Central.

TRANSFERENCIA DE DATOS VIA DISQUETE.

Como última solución, se maneja el envío de datos mediante la copia de los archivos en formato dbf hacia disquetes. Los mismos se enviarían conjuntamente con los formularios de las Declaraciones Juradas y se cargarían en el sistema de forma automática mediante la creación de un proceso para tal efecto.

4) – OTRAS SOLUCIONES A FUTURO

Una vez que se encuentre en funcionamiento el Sitio Web con todas sus funcionalidades, instalado, configurado, mantenido y administrado por personal del CETP, se pasaría a la etapa de implementación de conexión de las Escuelas en forma Online, las 24 horas del día.

Para ello se requerirá, en primer lugar, de la contratación e instalación de una tecnología de transmisión de datos que ofrezca servicio de banda ancha (ADSL) para cada una de las Escuelas. Como es de observarse, en la actualidad esto generaría altos costos en lo que refiere a contratación de líneas. En una primera etapa se podría comenzar con aquellas Escuelas que generan un cúmulo importante de datos y que presentan una gran problemática en su transferencia hacia el Sistema de Base de Datos Central de UTU, para más adelante extenderse en forma gradual hacia el resto de las Escuelas. De esta forma, serían posibles dos soluciones diferentes: (i) el ingreso de datos en cada Escuela con los sistemas informáticos ya existentes y su posterior transferencia hacia el Edificio Central de UTU (ii) la conexión online de las Escuelas las 24 horas del día, donde los sistemas informáticos existentes deberán ser desarrollados en la modalidad cliente-servidor. De este modo, las Escuelas se conectarán al sistema central de UTU, trabajando como si fuera un computador más de esta red, accediendo a la información directamente de la Base de Datos Central del sistema con la debida seguridad implementada. Los datos se manejarían en tiempo real, no siendo necesarios la administración y mantenimiento que presenta la transferencia de datos que se ha planteado hasta el momento. Se podría utilizar la red Internet como canal de comunicación para la transferencia de datos, mediante la creación de redes privadas virtuales que utilizan este medio para, mediante túneles, transferir los datos de forma confiable y segura. Esta solución es por supuesto muy ambiciosa.

4 Implementación

4.1 Situación Organizacional de UTU

La organización de UTU está estructurada en Programas[5] Educativos y de Gestión. Cada uno de los programas tiene sus respectivas subdivisiones. Los programas son:

- Recursos Humanos
  - Personal Docente
  - Personal No Docente
  - Junta Calificadora
- Financiero Contable
- Gestión Escolar.
  - Bedelía.
  - Designación Docente.
- Planeamiento Educativo.
- División Informática.

La División Informática de UTU, situada en el Edificio Central, consta de un departamento de programación encargado de desarrollar los sistemas informáticos necesarios para el correcto funcionamiento de la gestión del organismo.

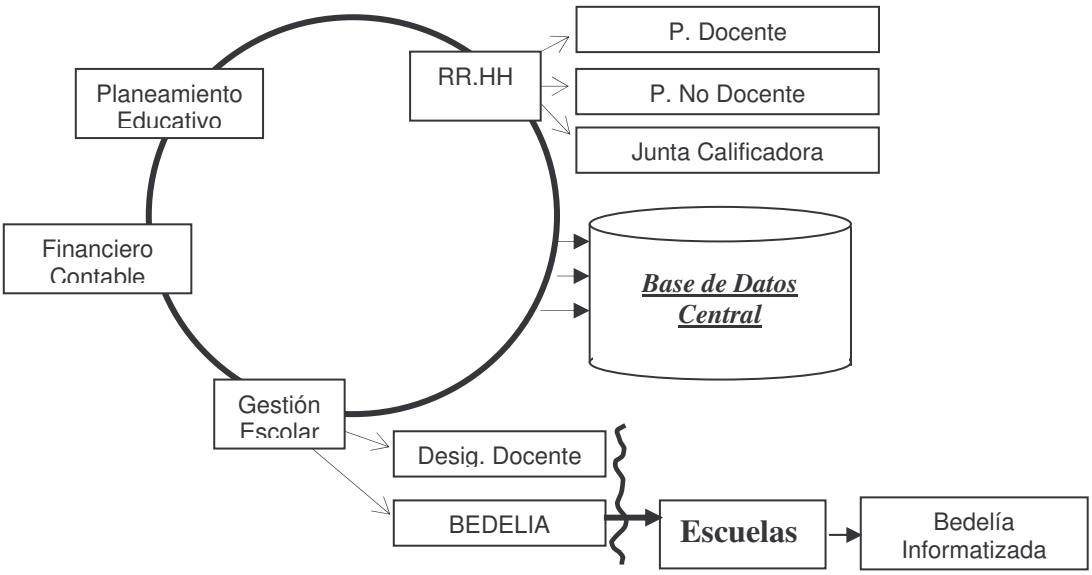


Fig. 9 – Esquema programas CETP

Actualmente, los desarrollos informáticos de UTU se encuentran en una etapa de transformación con el objetivo de unificar los datos de alumnos y docentes que se recaudan desde las diferentes Escuelas de Montevideo e Interior. Hasta el comienzo de esta migración, cada departamento poseía sus propios programas desarrollados en lenguaje Clipper, dando la posibilidad, y de hecho la existencia, de datos ambiguos e inconsistentes así como también su repetición en cada una de las oficinas.
Esta situación motivó el desarrollo de nuevos sistemas aplicando la herramienta Genexus, almacenando los datos en una ***Base de Datos Central*** en SQL Server 7.0.

[5] Debe destacarse que el término "Programa" es utilizado por el CETP como forma de referenciar a las diferentes divisiones departamentales que lo componen.

En la figura 9, se grafica el nivel de integración de los sistemas existentes en el CETP, en lo que a centralización de datos se refiere. Los programas que se encuentran sobre el círculo ejecutan sistemas desarrollados en el lenguaje de programación Genexus, centralizados en la base de datos central. El programa de gestión escolar se encarga de la gerencia las designaciones docentes así como los sistemas de bedelía informatizada que se ejecutan en las escuelas. Es aquí donde se ubica el módulo de declaraciones juradas, quien suministrará los datos referentes a las designaciones docentes transfiriéndolos directamente hacia la base de datos central para que queden accesibles a todos los programas de gestión.

A continuación se detallan las estructuras de los sistemas que componen la red informática de la UTU así como de las Escuelas.

Red Informática de UTU

La División Informática cuenta con varios Servidores instalados con Windows NT versión 4.0 sobre los cuales corre un Servidor de Base de datos MS-SQL Server 7.0 y el Servidor de Correo MS-Exchange. Se observa la existencia de una Intranet, corriendo bajo MS Internet Information Server. El desarrollo de sistemas se implementa mediante la herramienta Genexus corriendo bajo el sistema operativo Windows Server.

La red cuenta con sistemas de seguridad de la información establecidos bajo el inicio de sesión en Windows NT de todas las estaciones de trabajo que utilizan los sistemas informáticos desarrollados bajo Genexus. La red posee chequeo de antivirus Norton perfectamente instalado y en correcto funcionamiento.

Escuelas

La UTU cuenta con 94 escuelas, de las cuales 28 están en Montevideo.

La situación en las Escuelas es sumamente heterogénea: existen Escuelas que cuentan con redes informáticas para su gestión particular y otras que tienen un equipamiento informático mínimo (menos de 5 pc’s y menos de 3 impresoras).

Cabe destacar que todas las Reparticiones cuentan con al menos un equipo tipo PC de satisfactoria configuración. Algunas Escuelas (aproximadamente 4) no tienen disponibilidad de acceso a UruguayNet o Adinet, ya que están en medios rurales.

El software instalado en las Escuelas es el sistema operativo MS Windows 95/98 y utilizan para su gestión procesadores de texto, planillas electrónicas, etc..

Cada Escuela utiliza el Sistema de **Bedelía Informatizada** para recolectar los datos referentes a los cursos y actuaciones escolares de los alumnos inscriptos. Esta aplicación ya ha sido instalada en todas las escuelas del país, lo cual permite realizar el seguimiento de la tarea escolar. La comunicación para esta transferencia, se realiza a través del programa PcAnyWhere desde el Edificio Central hacia las Escuelas, no habiéndose encontrado un mecanismo fiable para que las mismas realicen una conexión hacia el Edificio Central. El uso del correo electrónico es inestable, por lo que ante inconvenientes reiterados, se desestimo por parte de la mayoría de las Escuelas.

Cabe mencionar que las Escuelas disponen de una línea telefónica con fines educativos, lo cual impide el acceso a Internet de forma continua.

4.2 Sistema de Declaraciones Juradas

Al momento de la implementación, se comenzó con el sistema de las Declaraciones Juradas. Se dejó pendiente el Sistema de Conectividad, dependiendo de UTU la selección del sistema que se adecuaría a los costos asociados a cada una de las soluciones presentadas.

Para el momento final de la implementación del Sistema de Declaraciones Juradas, UTU decidió que el envío de los datos correspondientes a las Declaraciones Juradas se realizará mediante disquete, quedando planteado para un futuro cercano, la concreción de la implementación del SitioWeb ó su conexión a Internet mediante ANEP.

El Sistema de Conectividad, en su etapa de implementación, queda entonces limitado a la implementación de la transferencia de datos hacia UTU que se desarrollará enviando los datos recopilados en disquetes, en formato dbf.

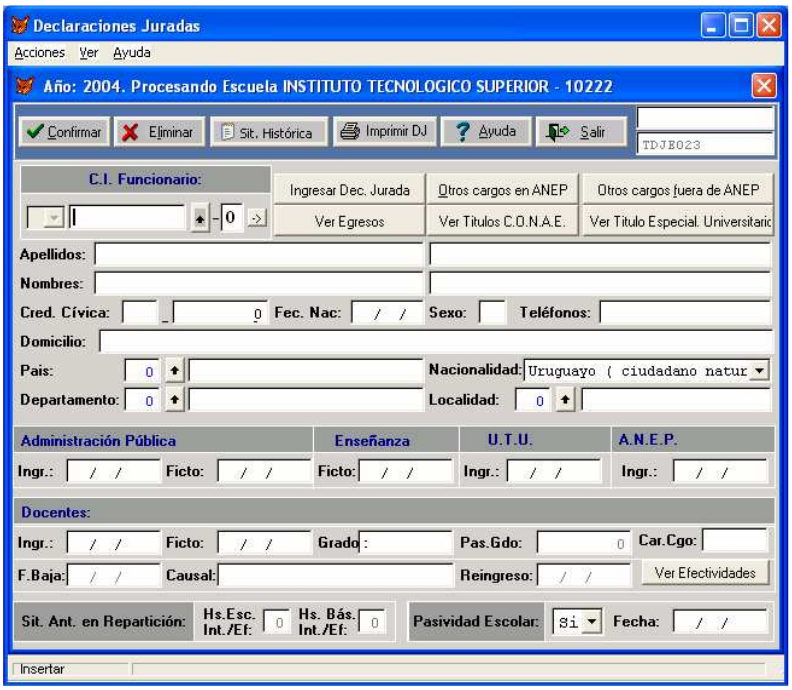
Se presenta a continuación el esquema de pantallas del sistema de Declaraciones Juradas.

4.3 Declaraciones Juradas - Esquema de Pantallas

La pantalla principal de ingreso al sistema es la siguiente:

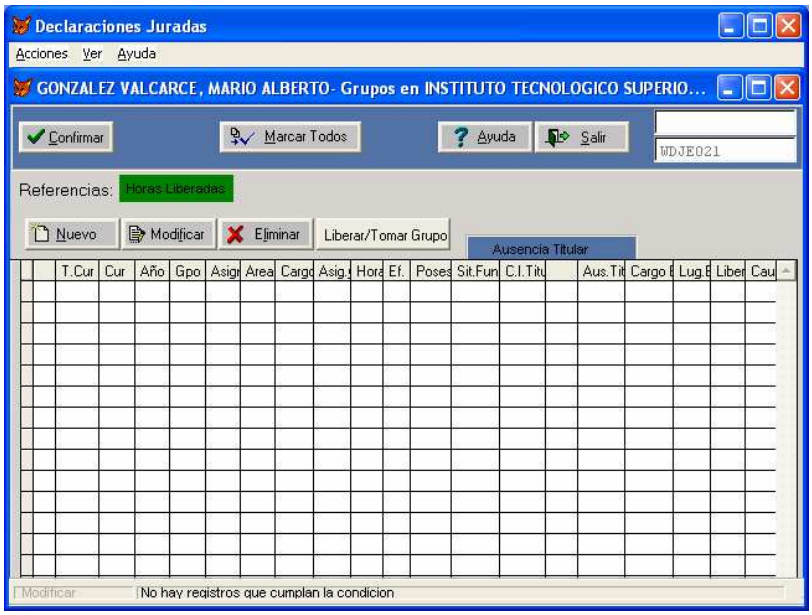
El usuario deberá iniciar sesión en el sistema, siendo el mismo nombre y contraseña que utiliza para el ingreso al sistema de Bedelía Informatizada. Una vez iniciada la sesión, se habilitarán las opciones de Ingreso de Declaraciones Juradas de esta Repartición o de Cursos Móviles que dependen de esta Repartición, y enviar los datos hacia el CETP que fueron recogidos en las Declaraciones Juradas ya ingresadas.

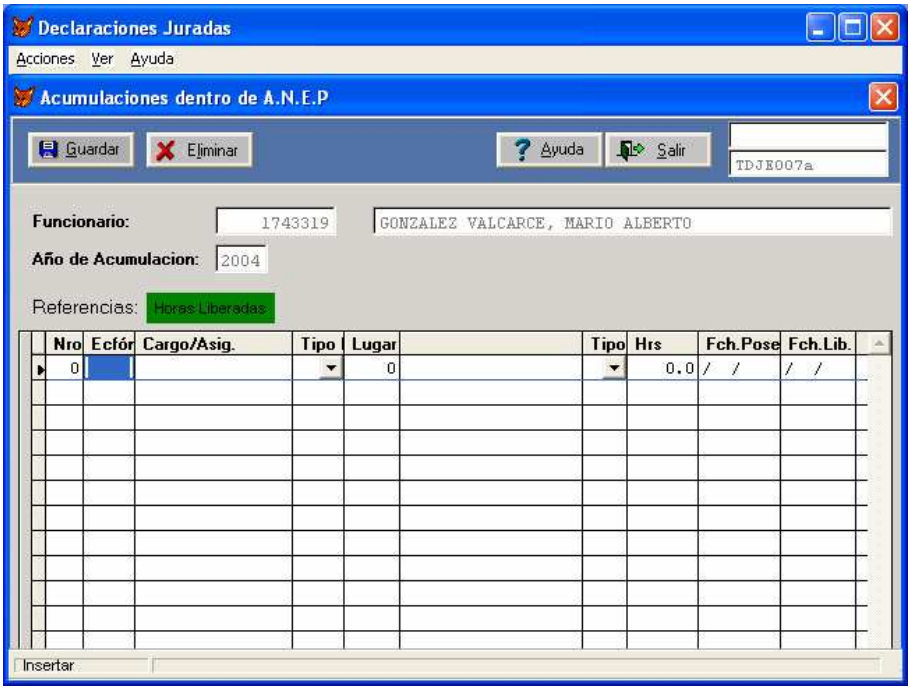
4.3.1 Ingresar Declaraciones Juradas de esta Repartición

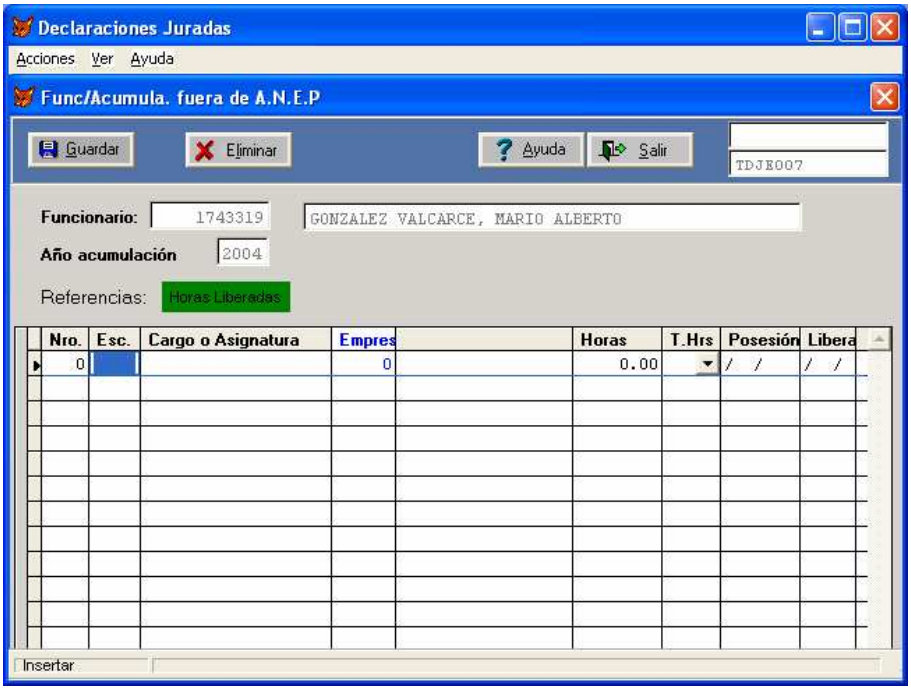


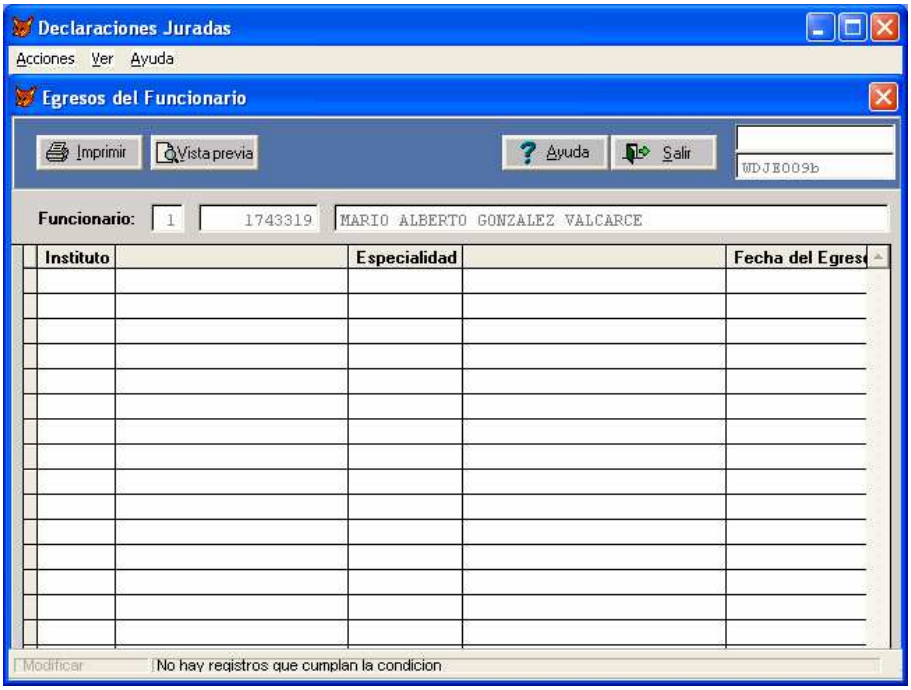
Si el funcionario docente ha dictado clases en esta Repartición aparecerán sus datos en pantalla para su posterior actualización si fuera necesario, de lo contrario será ingresado al sistema como un nuevo usuario. A continuación se habilita la posibilidad del ingreso de información referente a los cursos a los cuales el docente fue designado.

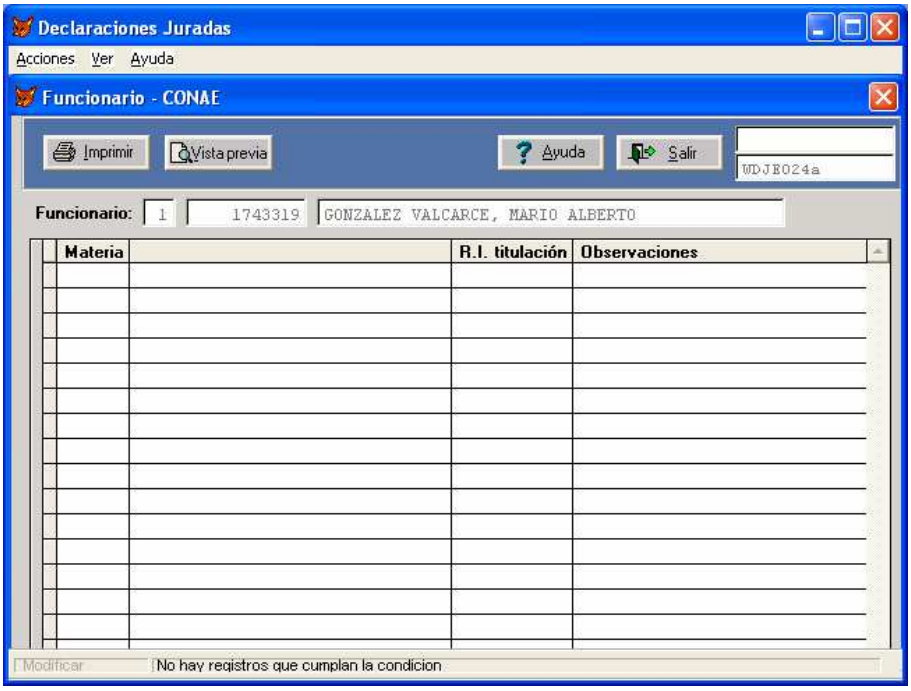
Si así es solicitado, será posible visualizar los cargos que este funcionario posee dentro y fuera de ANEP, títulos CONAE y universitarios y la información referente a los egresos. Todos estos datos serán transferidos al sistema por personal responsable del CETP, mediante listado electrónico emitido por el programa de Planeamiento Educativo.

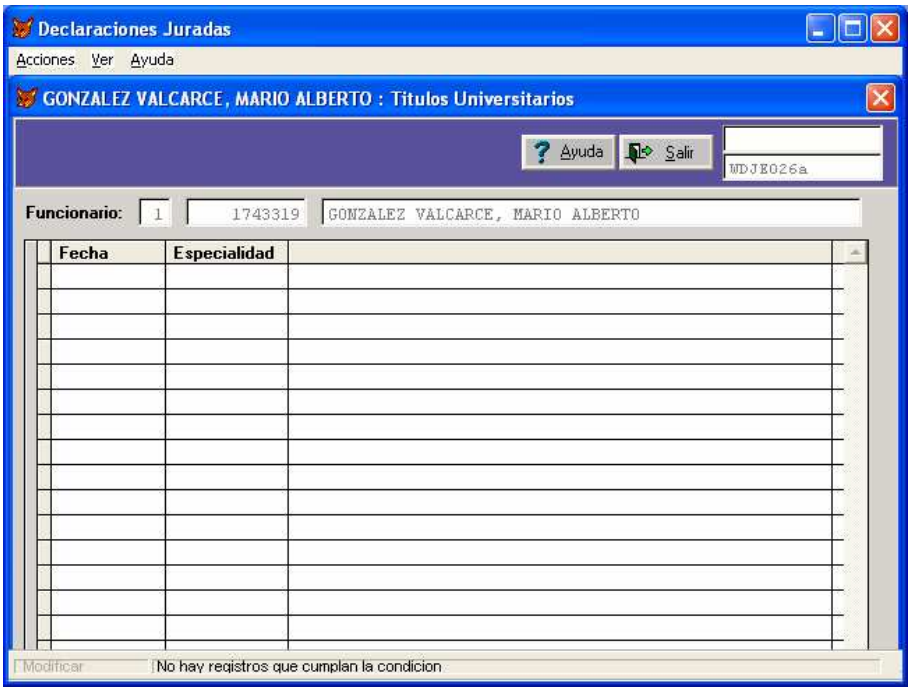



Declaraciones Juradas
Acciones Ver Ayuda
Acumulaciones dentro de A.N.E.P
Guardar
Eliminar
Ayuda
Salir
TDJE007a
Funcionario:
1743319
GONZALEZ VALCARCE, MARIO ALBERTO
Año de Acumulacion:
2004
Referencias:
Horas Liberadas
Nro
Ecfór
Cargo/Asig.
Tipo
Lugar
Tipo
Hrs
Fch.Pose
Fch.Lib.
0
0.0
/ /
/ /
Insertar


Declaraciones Juradas
Acciones Ver Ayuda
Func/Acumula. fuera de A.N.E.P
Guardar
Eliminar
Ayuda
Salir
TDJE007
Funcionario:
1743319
GONZALEZ VALCARCE, MARIO ALBERTO
Año acumulación
2004
Referencias:
Horas Liberadas
Nro.
Esc.
Cargo o Asignatura
Empres
Horas
T.Hrs
Posesión
Libera
0
0.00
/ /
/ /
Insertar

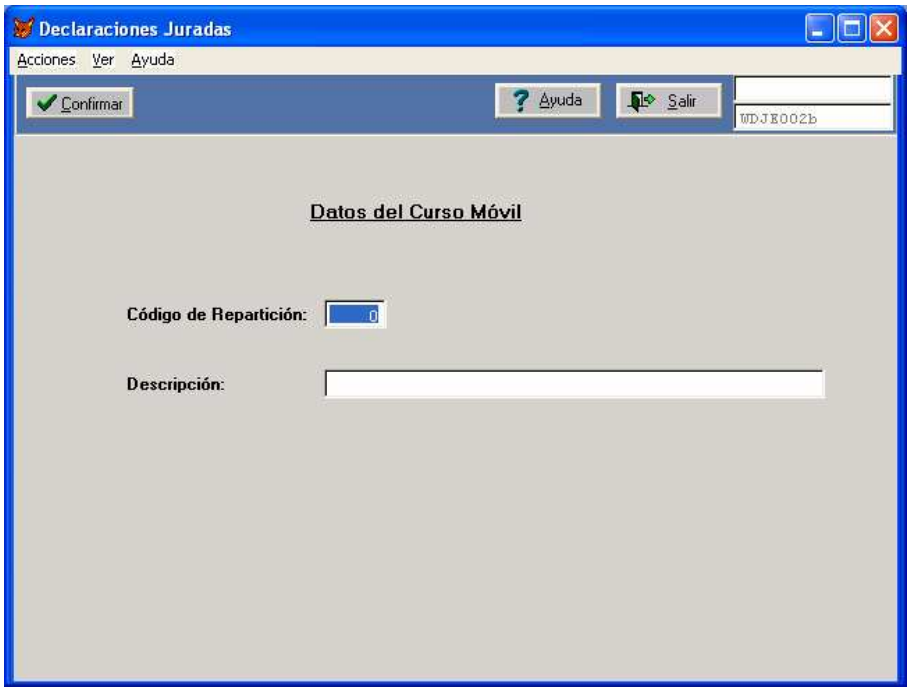

Declaraciones Juradas
Acciones Ver Ayuda
Egresos del Funcionario
Imprimir
Vista previa
Ayuda
Salir
WDJE009b
Funcionario:
1
1743319
MARIO ALBERTO GONZALEZ VALCARCE
Instituto
Especialidad
Fecha del Egres
Modificar
No hay registros que cumplan la condicion


Declaraciones Juradas
Acciones Ver Ayuda
Funcionario - CONAE
Imprimir
Vista previa
Ayuda
Salir
WDJE024a
Funcionario:
1
1743319
GONZALEZ VALCARCE, MARIO ALBERTO
Materia
R.I. titulación
Observaciones
Modificar
No hay registros que cumplan la condicion



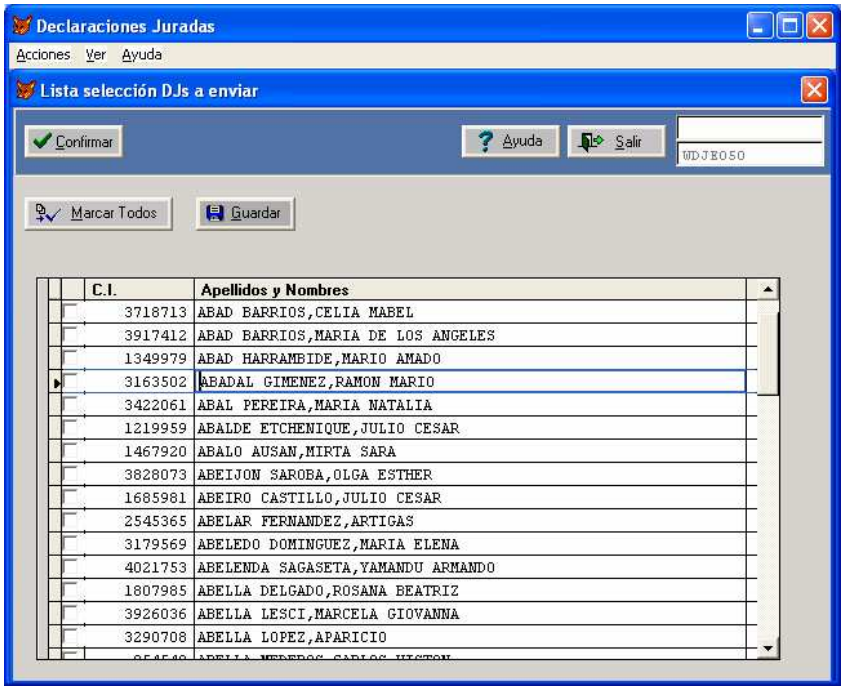
4.3.2 Cursos Móviles

Se consideran cursos móviles aquellos cursos que dependiendo de una Repartición son dictados fuera de la misma, por ejemplo cursos en las cárceles. Una Repartición sólo podrá ingresar Declaraciones Juradas de cursos que dependan de ella, por lo tanto antes de iniciar la Declaración Jurada del docente, se realizan estos controles.



Al confirmar se ingresa a la pantalla de ingreso de Declaraciones Juradas.

4.3.3 Envío de datos hacia el CETP



El usuario deberá seleccionar el o los nombres dentro de la lista de funcionarios, de quienes desea enviar los datos hacia el CETP. Una vez que los funcionarios han sido elegidos, se confirman y se envian a disquete mediante el botón Guardar.

5 Conclusiones

La situación actual de desarrollo de los sistemas informáticos de UTU muestra que los problemas administrativos son resueltos con ayuda del computador pero no en forma integrada, esto soluciona necesidades locales particulares sin que el impacto de las mismas haya tenido como principal logro una mejora significativa en el funcionamiento global.

Como se ha mencionado anteriormente en este documento, la comunicación entre las Escuelas y el Edificio Central, en lo que a distribución de la información se refiere, ha presentado muchos inconvenientes y hasta el fracaso de los sistemas que existían. Tras el desarrollo del sistema de Bedelía Informatizada, que se encuentra en funcionamiento en las Escuelas, se continúan observando dificultades en el manejo de la información que se transfiere desde las Escuelas hacia el Edificio Central y viceversa.

Hasta el momento en que se desarrolla el presente proyecto, las Declaraciones Juradas se ingresan de forma manual, para luego ser enviadas a diferentes departamentos, donde los mismos datos son procesados más de una vez e ingresados en sistemas diferentes, en varios casos. El desarrollo del sistema de Declaraciones Juradas implementado en el presente proyecto, además de solucionar la problemática existente en la consulta y transferencia de datos correspondiente a asignaciones docentes, brinda a la Institución un mecanismo para la unificación de datos de forma consistente, ahorrando tiempo de proceso y procesamiento de los datos.

Permitir el acceso desde las Escuelas a la Intranet de UTU permitirá mantener la red Organizacional en forma privada con altos niveles de confiabilidad en cuanto a la seguridad y privacidad de los datos que por ella circulan. Cada vez son más los usuarios de computadoras que se familiarizan con la navegación por Internet y el manejo dentro de la red, por lo que manejarse dentro de una Intranet no ocasiona dificultades ni requiere muchas horas de capacitación, dado que la interfase operativa es la misma. Por otro lado, el contrato de una línea digital dedicada en el CETP (el estudio de costos no se ha presentado en este documento) permitiría establecer la presencia de dicha Institución en Internet, brindando la posibilidad de que las Escuelas puedan acceder a dicha Intranet en las condiciones deseadas.
Otro de los aspectos significativos en este punto de la implementación de la conectividad se da en la infraestructura de los “clientes” (en este caso las Escuelas), el cual todavía no se ha solucionado. Se espera que en el futuro, ANEP establezca la conectividad de cada una de las Escuelas, habilitando el acceso a Internet ya sea por acceso directo o discado. El CETP presenta como una solución a futuro la conexión de una línea dedicada las 24 horas que permita el acceso directo a la red del CETP, vía Internet, pudiéndose acceder de forma inmediata y online, brindando de esta manera una mejora sustancial en el acceso a datos, no solamente los referentes a las Declaraciones Juradas, sino también a otros datos que el CETP considere.

El CETP, al momento de finalización del presente proyecto, ha analizado las posibles soluciones de conectividad presentadas, y de acuerdo al estudio de factibilidad, ha decidido que la transferencia de datos entre las Escuelas y el CETP se realice mediante disquetes. Seguramente esta es la solución tecnológicamente de menor relevancia, pero es la que la UTU actualmente está en condiciones de poner en práctica. El desarrollo promovido por este documento permite que la solución adoptada por la Institución sea escalable (se comienza con lo más necesario y se va construyendo de acuerdo con las necesidades). Cuando sea

implementada la presencia del CETP en Internet, será posible ir ampliando desde las Escuelas la transferencia remota de datos que alimentan la Base de Datos Central de UTU. Queda aún por implementar la presencia institucional del CETP en Internet, con la consecuente creación de un sistema de publicación y consulta de datos en Internet.

En síntesis, se ha desarrollado un sistema para el ingreso de Declaraciones Juradas a ejecutarse en las Escuelas integrado al sistema de Bedelía Informatizada ya existente. El sistema envía los datos que recopila hacia el Edificio Central de UTU mediante archivos dbf en disquetes, cumpliéndose los objetivos que no dependieron de la implementación de la conectividad. Además se ha realizado en el presente proyecto un estudio de conectividad que posibilitará, en un futuro, la presencia de UTU en Internet así como la eventualidad de implementar nuevos mecanismos para la transferencia de datos desde y hacia las Escuelas en forma más confiable y segura.

Queda aún pendiente el desarrollo de un sistema para la introducción de datos en la Base Central de UTU debido a que la Institución aún no ha decidido las pautas en cuanto al mecanismo de inserción de los mismos: un proceso automático ó un proceso bajo supervisión humana que cheque los datos contra la copia en papel de la Declaración Jurada docente y los inserte en la base de datos central.

6 Proyecciones a Futuro

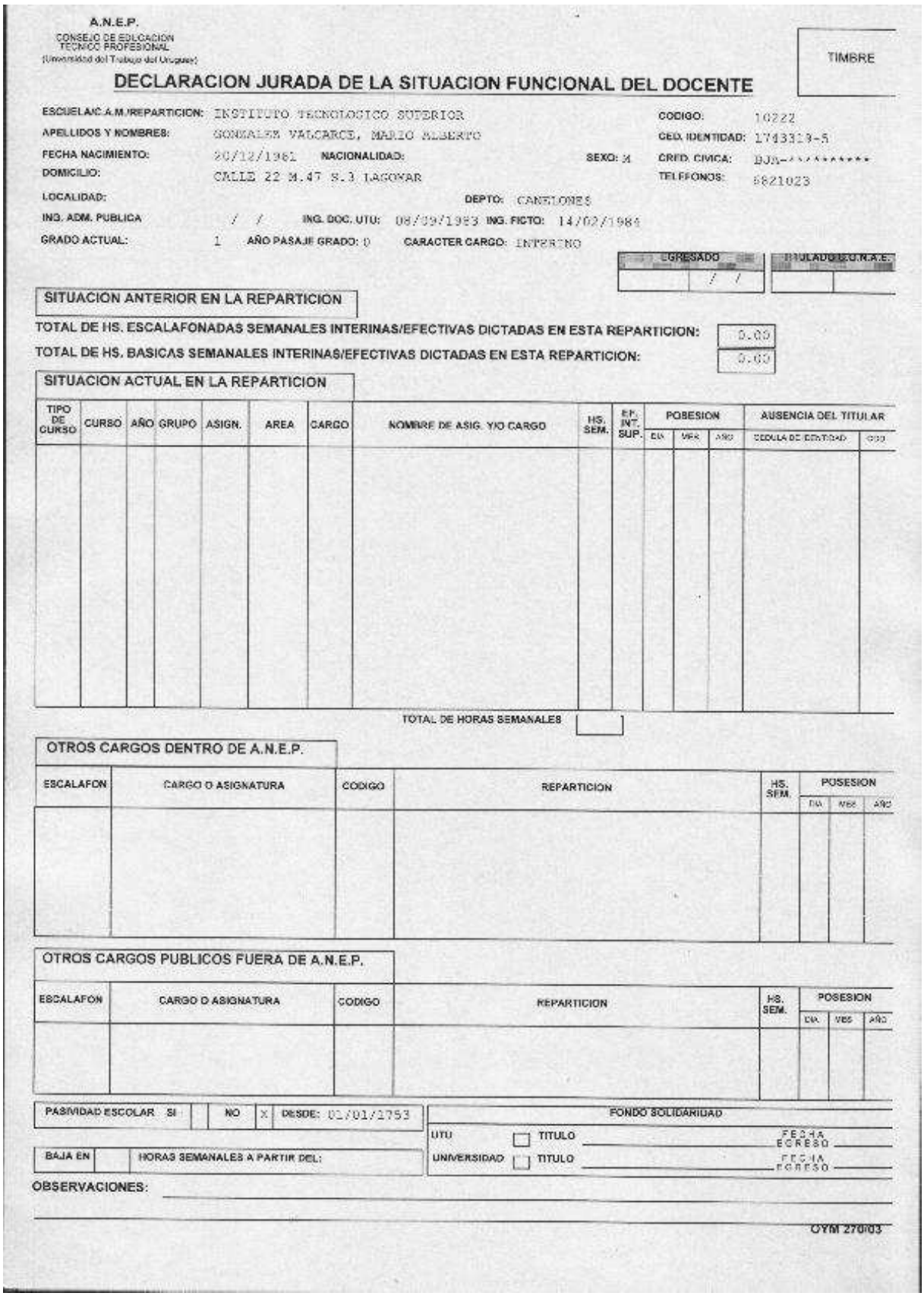
Queda mucho camino por recorrer.

En el corriente año lectivo, se pondrá en uso el programa de Declaraciones Juradas en 4 escuelas del Interior. Aún queda pendiente llevarlo a todas las escuelas de Montevideo, y no menos importante, poder instalarlo en todas las escuelas del Interior del País.

Queda aún pendiente la definición de un sistema de transferencia de datos que minimice la pérdida de datos y que brinde buena eficiencia, requiriendo el menor esfuerzo por parte de los usuarios que manejan el sistema de Bedelía Informatizada y el Sistema de Base de Datos Central (en el Edificio Central de UTU). Es un objetivo vital para el CETP el implementar una solución de transferencia de datos vía Internet, que deposite los datos en un lugar físico dentro de un servidor, y que luego de forma automática estos datos sean incorporados hacia el sistema central de UTU.

La implementación del Sitio Web ha quedado pendiente en su totalidad dependiendo en gran medida de las autoridades de la Institución así como de la evolución de las diferentes tecnologías que van surgiendo día a día, dejando obsoletas muchas de las soluciones que se pueden haber planteado y abriendo otras nuevas posibilidades, que deberán ser motivo de posterior análisis.

Apéndice A: Formulario de Declaraciones Juradas



A.N.E.P.
CONSEJO DE EDUCACION TECNICO PROFESIONAL
(Universidad del Trabajo del Uruguay)

TIMBRE

DECLARACION JURADA DE LA SITUACION FUNCIONAL DEL DOCENTE

ESCUELA/C.A.M./REPARTICION: INSTITUTO TECNOLOGICO SUPERIOR — CODIGO: 10222
APELLIDOS Y NOMBRES: GONZALEZ VALCARCE, MARIO ALBERTO — CED. IDENTIDAD: 1743319-5
FECHA NACIMIENTO: 20/12/1961 NACIONALIDAD: SEXO: M CRED. CIVICA: BJA-*/*/******
DOMICILIO: CALLE 22 N.47 E.3 LAGOMAR — TELEFONOS: 6821023
LOCALIDAD: DEPTO: CANELONES
ING. ADM. PUBLICA / / ING. DOC. UTU: 08/09/1983 ING. FICTO: 14/02/1984
GRADO ACTUAL: 1 AÑO PASAJE GRADO: 0 CARACTER CARGO: INTERINO

EGRESADO	TITULADO I.S.T.U./C.E.T.P.
/ /	

SITUACION ANTERIOR EN LA REPARTICION

TOTAL DE HS. ESCALAFONADAS SEMANALES INTERINAS/EFECTIVAS DICTADAS EN ESTA REPARTICION: 0.00
TOTAL DE HS. BASICAS SEMANALES INTERINAS/EFECTIVAS DICTADAS EN ESTA REPARTICION: 0.00

SITUACION ACTUAL EN LA REPARTICION

TIPO DE CURSO	CURSO	AÑO	GRUPO	ASIGN.	AREA	CARGO	NOMBRE DE ASIG. Y/O CARGO	HS. SEM.	EP. INT. SUP.	POSESION DIA	POSESION MES	POSESION AÑO	AUSENCIA DEL TITULAR CEDULA DE IDENTIDAD	AUSENCIA DEL TITULAR CGO

TOTAL DE HORAS SEMANALES

OTROS CARGOS DENTRO DE A.N.E.P.

ESCALAFON	CARGO O ASIGNATURA	CODIGO	REPARTICION	HS. SEM.	POSESION DIA	POSESION MES	POSESION AÑO

OTROS CARGOS PUBLICOS FUERA DE A.N.E.P.

ESCALAFON	CARGO O ASIGNATURA	CODIGO	REPARTICION	HS. SEM.	POSESION DIA	POSESION MES	POSESION AÑO

PASIVIDAD ESCOLAR SI [ ] NO [X] DESDE: 01/01/1753

FONDO SOLIDARIDAD

BAJA EN [ ] HORAS SEMANALES A PARTIR DEL:

UTU [ ] TITULO _____ FECHA EGRESO _____
UNIVERSIDAD [ ] TITULO _____ FECHA EGRESO _____

OBSERVACIONES:

OYM 270/03

NOTA: Art. 239 del Código Penal: "Falsificación ideológica por un particular. El que con motivo del otorgamiento o formalización de un documento público, ante un funcionario público, presente una declaración falsa sobre su identidad o estado o cualquiera otra circunstancia de hecho, será castigado con tres a veinticuatro meses de prisión.

DECLARO BAJO JURAMENTO: que la situación del docente que antecede, es la real, a la fecha, en esta Escuela. Me comprometo a sustituir de inmediato esta declaración, si cambiara cualquier dato de la misma.	DECLARO BAJO JURAMENTO: que la que antecede es la situación real, de los cargos públicos y otras situaciones, aún las en trámite de acumulación y pasividades a la fecha. Me comprometo a sustituir de inmediato esta declaración, si cambiara cualquier dato de la misma, por intermedio de esta Escuela.
Firma del Director	Firma del Docente

LOCALIDAD Y FECHA EN QUE SE FIRMA:

NORMAS:

- Documentos a presentar al Departamento de Personal Docente, por el docente recién ingresado o que reingresa al Consejo de Educación Técnico Profesional: Carné de Salud, Credencial Cívica o Carta de Ciudadanía, Certificado de Juramento de Fidelidad a la Bandera, 3 Fotos carné.
- El docente no podrá presentar ninguna reclamación relativa a sus haberes en División Hacienda, sin exhibir su declaración que la fundamente. Esta le será entregada en la Escuela y deberá mantenerla en su poder.
- El docente que cumpla funciones en mas de una Escuela tendrá una declaración por cada una de ellas, por las respectivas horas trabajadas.
- Para el pago de los haberes es indispensable que el docente entregue toda documentación que se solicita y en su caso, concluya su trámite de acumulación de cargos y sueldos.
  Se extiende en 4 vías, todas firmadas y perfectamente legibles. Una vía debe entregarse al docente.
- Se utilizarán 5 vías para cuando se trata de Docentes con cargo básico y hs. escalafonadas.
- Si algún dato impreso fuera erróneo, se debe aclarar en el espacio destinado a observaciones.
- El formulario original debe contener Timbre de Caja de Profesionales Universitarios.
- Cuando se esté efectuando una suplencia se debe agregar el número de cédula del Docente Titular y el código de los motivos de ausencia.
- Si el docente ingresa al Consejo de Educación Técnico Profesional deberá adjuntar dos fotocopias de la cédula de identidad.
- Si el docente ingresa a la Institución y es egresado de alguno de los Institutos de Formación Docente o Profesional Universitario agregar fotocopia autenticada del Título.

DEPARTAMENTO DE PERSONAL DOCENTE

RECEPCION EN SECTOR DECLARACIONES DOCENTES CON FECHA:

DATOS INGRESADOS AL COMPUTADOR CON FECHA:

PASE A SECTOR CARPETAS PARA SU ARCHIVO CON FECHA:

Firma del Procesador

DIVISION HACIENDA

RECEPCION EN LA SECCION LIQUIDACION DE SUELDOS CON FECHA:	LIQUIDADO CON PRESUPUESTO DE DE ALTA CON PRESUPUESTO DE DE SUELDO EN SUSPENSO SI ☐ NO ☐
Firma del Jefe o Verificador	Liquidador / Verificador

Apéndice B – Diseño de Base de Datos

Tabla **Grupos** (ACEGru)

	Nombre	Descripción	Tipo
✯	AcuAle	Año Lectivo	N (4.0)
✯	ACuSLe	Semestre Lectivo	N (2.0)
✯	PlaCod	Código de Plan	C (4)
✯	TcuCod	Código de Tipo de Curso	C (3)
✯	CurCod	Código de Curso	C (3)
✯	ACuAAA	Año dentro del Curso	N (2.0)
✯	AcuSem	Semestre dentro del Curso	N (2.0)
✯	RepCod	Código de Repartición	N (5.0)
✯	GruCod	Código de Grupo	C (3.0)
	TurCod	Código de Turno	N (1.0)
	GruDCT	Días de clase teóricas	N (3.0)
	GruUsuDes	Nombre del Usuario	C (15)
	GruUsuFec	Fecha de actualización de datos	D
	GruUsuHor	Hora de actualización de datos	C (8)

Tabla **Grupos de Planeamiento** (AceGrp)

	Nombre	Descripción	Tipo
✯	AcuAle	Año Lectivo	N (4.0)
✯	ACuSLe	Semestre Lectivo	N (2.0)
✯	PlaCod	Código de Plan	C (4)
✯	TcuCod	Código de Tipo de Curso	C (3)
✯	CurCod	Código de Curso	C (3)
✯	ACuAAA	Año dentro del Curso	N (2.0)
✯	AcuSem	Semestre dentro del Curso	N (2.0)
✯	RepCod	Código de Repartición	N (5.0)
✯	GrpCod	Código de Grupo	C (3.0)
	GrpDes	Descripción del Grupo	C (2)
	TurCod	Código de Turno	N (1.0)
	ACEGrpMar	ACEGrpMar	C (1)
	ACEGrpCAl	ACEGrpCAl	N (3.0)
	ACEGrpFAl	Fecha de alta en ACEGRP	D
	ACEGrpBa	Fecha de baja en ACEGRP	D
	ACEGrpHAs	Horas asignadas al grupo	N (5.1)

Tabla **Reparticiones del CETP (Repart)**

	Nombre	Descripción	Tipo
✯	RepCod	Código de Repartición	N (5.0)
	RepDes	Nombre de la Repartición	C (50)
	RepAbr	Nombre común abreviado	C (15)
	RepCodHac	Codigo de Repartición de Hacienda	N (3.0)
	TReCod	Código de tipo de repartición	N (2.0)
	RepInRUlt	Ult. Núm. Inventario en Repartición	N (10.0)
	DepCod	Código de Departamento	N (2.0)

	RepRelJer	Relación Jerárquica	N (5.0)
	RepDirCll	Calle de la Repartición	C (30)
	RepDirNro	Nro. de calle de la Repartición	C (10)
	RepTel	Teléfono de la Repartición	C (25)
	RepAudUsu	Usuario que modifica	C (20)
	RepAudFec	Fecha en que se modifica	D
	RepAudHor	Hora en que se modifica	C (8)

Tabla **Maestro de Departamentos (Depart)**

	Nombre	**Descripción**	**Tipo**
✯	DepCod	Código de departamento	N (2.0)
	DepDes	Nombre de Departamento	C (15)
	DepAbr	Nombre común abreviado	C (3)
	DepAudUsu	Usuario que modifica	C (20)
	DepAudFec	Fecha en que se modifica	D
	DepAudHor	Hora en que se modifica	C (8)

Tabla **Maestro de Tipo de Reparticion (TipRep)**

	Nombre	**Descripción**	**Tipo**
✯	TReCod	Código de Tipo de Repartición	N (2.0)
	TreDes	Nombre de Tipo de Repartición	C (40)

Tabla **Areas de Asignaturas (Areas)**

	Nombre	**Descripción**	**Tipo**
✯	AreCod	Código de Area	C (5)
	AreDes	Descripción de Area	C (35)
	AreAbr	Descripción de Area Abreviada	C (16)
	AreCat	Areas por Categorías	C (1)
	AreEscCat	Indicador orden categorías en escalafón	C (1)
	AreAudUsu	Usuario que modifica	C (20)
	AreAudFec	Fecha en que se modifica	D
	AreAudHor	Hora en que se modifica	C (8)

Tabla **Materias (Materias)**

	Nombre	**Descripción**	**Tipo**
✯	MatCod	Código de Materia	C (5)
	MatDes	Descripción de Materia	C (35)
	MatAbr	Descripción Abreviada de la Materia	C (16)
	MatAudUsu	Usuario que modifica	C (20)
	MatAudFec	Fecha en que se modifica	D
	MatAudHor	Hora en que se modifica	C (8)

Tabla **Cursos (Cursos)**

	Nombre	Descripción	Tipo
✯	CurCod	Código de Curso	C (3)
	CurDes	Descripción de Curso	C (35)
	CurAbr	Curso Descripción Abreviada	C (16)
	CurGrpCod	Identificador de Grupo	C (2)
	CurAudUsu	Usuario que modifica	C (20)
	CurAudFec	Fecha en que se modifica	D
	CurAudHor	Hora en que se modifica	C (8)

Tabla **Tipos de Cursos (TipCur)**

	Nombre	Descripción	Tipo
✯	TcuCod	Código de Tipo de Curso	C (3)
	TcuDes	Descripción de Tipo de Curso	C (35)
	TcuAbr	Descripción Abreviada de Tipo de Curso	C (16)
	TcuAudUsu	Usuario que modifica	C (20)
	TcuAudFec	Fecha en que se modifica	D
	TcuAudHor	Hora en que se modifica	C (8)

Tabla **Planes de Estudio (Planes)**

	Nombre	Descripción	Tipo
✯	PlaCod	Código de Plan	C (4)
	PlaDes	Descripción de Plan	C (30)
	PlaRCoFec	Fecha de Resolución	D
	PlaRCoAct	Acta Resolución	N (4.0)
	PlaRCoNot	Nota Resolución	N (5.0)
	PlaAudUsu	Usuario que modifica	C (20)
	PlaAudFec	Fecha en que se modifica	D
	PlaAudHor	Hora en que se modifica	C (8)

Tabla **Funcionarios (Funcio)**

	Nombre	Descripción	Tipo
✯	TDICod	C. Tipo de Identidad	N (2.0)
✯	FunCod	Documento de Identidad	C (11)
	FunSex	Sexo	C (1)
	FunFNa	Fecha de Nacimiento	D
	PaiCod	Código de País	N (3.0)
	FunNac	Nacionalidad	N (1.0)
	FunCCiSer	Credencial Cívica (Serie)	C (3)
	FunCCiNro	Credencial Cívica (Número)	N (6.0)
	EcvCod	Código de Estado Civil	N (2.0)
	DepCod	Código de Departamento	N (2.0)
	LocCod	Código de Localidad	N (3.0)
	FunDir	Dirección	C (50)
	FunTel	Teléfonos	C (25)
	FunFInAPu	Fecha de Ingreso a la Adm. Pública	D

	FunFinAne	Fecha de Ingreso ANEP	D
	FunFinDoc	Fecha de Ingreso a la docencia	D
	FunFinNDo	Fecha de Ingreso a la No docencia	D
	FunFFiDoc	Fecha ficta docente	D
	FunFFiNDo	Fecha ficta no docente	D
	FunFinUTU	Fecha de ingreso a UTU	D
	FunFFiAPu	Fecha Ficta Administración Pública	D
	FunCDV	Dígito Verificador	N (1.0)
	FunAp1	Primer Apellido Funcionario	C (20)
	FunAp2	Segundo Apellido Funcionario	C (20)
	FunNo1	Primer Nombre	C (20)
	FunNo2	Segundo Nombre	C (20)
	FunFFiEns	Fecha Ficta de Ingreso a la Enseñanza	D
	FunFBaDoc	Fecha de Baja a la Docencia	D
	FunFReDoc	Fecha de Reingreso a la Docencia	D
	FunPasEsc	Indicador de pasividad escolar	C (1)
	FunPEsFec	Fecha de la pasividad escolar	D
	FunCBaDoCo	Código Causal de baja en la docencia	N (3.0)
	FunActUsu	Usuario que modifica	C (20)
	FunActFec	Fecha en que se modifica	D
	FunActHor	Hora en que se modifica	

Tabla **Grupos del Funcionario** (FunGru)

	Nombre	**Descripción**	**Tipo**
✯	TDICod	C. Tipo de doc. De Identidad	N (2.0)
✯	FunCod	Documento de Identidad	C (11)
✯	AcuALe	Año Lectivo	N (4.0)
✯	AcuSLe	Semestre Lectivo	N (2.0)
✯	TcuCod	Código de Tipo de Curso	C (3)
✯	CurCod	Código de Curso	C (3)
✯	PlaCod	Código d Plan	C (4)
✯	ACuAAA	Año dentro del Curso	N (2.0)
✯	AcuSem	Semestre dentro del Curso	N (2.0)
✯	RepCod	Código de Repartición	N (5.0)
✯	GrpCod	Código de Grupo	C (3)
✯	MatCod	Código de Materia	C (5)
✯	TcaCod	Código de Tipo de Curso	N (1.0)
✯	CarCod	Código de Cargo	C (4)
✯	FgrFPo	Fecha de posesión	D
✯	FgrSFuTit	Código de Situación Funcional Titular	N (3.0)
	FgrHor	Horas semanales	N (5.2)
	FgrCCgCod	Código Car.Cargo hrs. Fun/Grupo	C (1)
	FgrFLi	Fecha de liberación de Grupo	D
	FGrTitTDI	Cód. Tipo Doc. ID. Titular de horas	N (2.0)
	FgrTitCod	Código de Funcionario del Titular	C (11)
	FgrTCaExo	Tipo cargo por el cual exonera	N (1.0)
	FgrLugExo	Código Lugar exoneración horas	N (5.0)
	FgrAudUsu	Usuario que modifica	C (20)
	FgrAudFec	Fecha en que se modifica	D
	FgrAudHor	Hora en que se modifica	C (8)

Tabla **Cargos Docentes y no Docentes (cargos)**

	Nombre	Descripción	Tipo
✯	TcaCod	Código de Tipo de Cargo	N (1.0)
✯	CarCod	Código de cargo	C (4)
	CarDes	Descripción del cargo	C (30)
	CarAbr	Descripción abreviada del cargo	C (5)
	CarFCr	Fecha de creación	D
	CarFCa	Fecha de cancelación	D
	CarHrs	Horas asignadas al cargo	N (2.0)
	CarAudUsu	Usuario que modifica	C (20)
	CarAudFec	Fecha en que se modifica	D
	CarAudHor	Hora en que se modifica	C (8)

Tabla **Escalafones (Escalafo)**

	Nombre	Descripción	Tipo
✯	Tcacod	Código de Tipo de Cargo	N (1.0)
✯	EscCod	Código de Escalafón	C (1)
	EscDes	Descripción del Escalafón	C (35)
	EscAudUsu	Usuario que modifica	C (20)
	EscAudFec	Fecha en la que se modifica	D
	EscAudHor	Hora en la que se modifica	C (8)

Tabla **Grados (Grados)**

	Nombre	Descripción	Tipo
✯	TcaCod	Código de Tipo de Cargo	N (1.0)
✯	CarCod	Código de Cargo	C (4)
	GraCod	Código de Grado	C (3)
	GraDes	Descripción de Grado	C (20)
	GraAbr	Descripción Abreviada del Grado	C (5)
	GraAudUsu	Usuario que modifica	C (20)
	GraAudFec	Fecha en que se modifica	D
	GraAudHor	Hora en que se modifica	C (8)

Tabla **Caracteres de Cargo (CarCargo)**

	Nombre	Descripción	Tipo
✯	CarCgoCod	Código de Caracter de Cargo	N (2.0)
	CarCgoDes	Descripción de Caracter de Cargo	C (20)
	CarCgoAbr	Abreviatura de Caracter de Cargo	C (5)
	CarCgoAUsu	Usuario que modifica	C (20)
	CarCgoAFec	Fecha en que se modifica	D
	CarCgoAHor	Hora en que se modifica	C (8)

Tabla **Titulaciones CONAE del Funcionario (FTiCONAE)**

	Nombre	Descripción	Tipo
✯	TDICod	C. Tipo de Doc. De Identidad	N (2.0)
✯	FunCod	Documento de Identidad	C (11)
✯	FTCMatCod	Materia titulación CONAE	C (5)
	FTCR_I	R.I de la titulación CONAE	C (10)
	FTCObs	Observaciones de la titulación CONAE	C (80)

Tabla **Acumulacion Dentro de ANEP (FDAnep)**

	Nombre	Descripción	Tipo
✯	TDICod	C.Tipo de Doc. De Identidad	N (2.0)
✯	FunCod	Documento de Identidad	C (11)
✯	FADAANEAAA	Año de Acumulación en ANEP	N (4.0)
✯	FAANELin	Nro. De linea en las acumulaciones	N (3.0)
	FADANETLu	Tipo-Lugar (Repartición-Emp. Pública)	C (1)
	FADANELug	Código Lugar Acumulado en ANEP	N (5.0)
	FADANEFPo	Fecha de Posesión Acumu. en ANEP	D
	FADANEEcf	Escalafón acum. Dentro ANEP	C (1)
	FADANECAs	Cargo/Asig. Acumulación ANEP	C (35)
	FADANEHTi	Tipo de Hrs.Acum: ANEP	C (1)
	FADANEHrs	Cant. Horas Acum. ANEP	N (4.1)
	FADANEFLI	Fecha liberación	D

Tabla **Acumulacion Fuera de ANEP (FFAnep)**

	Nombre	Descripción	Tipo
✯	TDICod	C.Tipo de Doc. De Identidad	N (2.0)
✯	FunCod	Documento de Identidad	C (11)
✯	FAFAANEAAA	Año de Acumulación fuera ANEP	N (4.0)
✯	FAFANELin	Nro. De linea en las acumulaciones	N (3.0)
	FAFANEEpr	Empresa acumula fuera ANEP	N (5.0)
	FAFANEFPo	Fecha de Posesión Acumu. Fuera ANEP	D
	FAFANEEcf	Escalafón acum. fuera ANEP	C (1)
	FAFANECAs	Cargo/Asig. Acumulación fuera ANEP	C (35)
	FAFANEHTi	Tipo de Hrs.Acum: fuera ANEP	C (1)
	FAFANEHrs	Cant. Horas Acum.fuera ANEP	N (4.1)
	FAFANEFLI	Fecha liberación	D

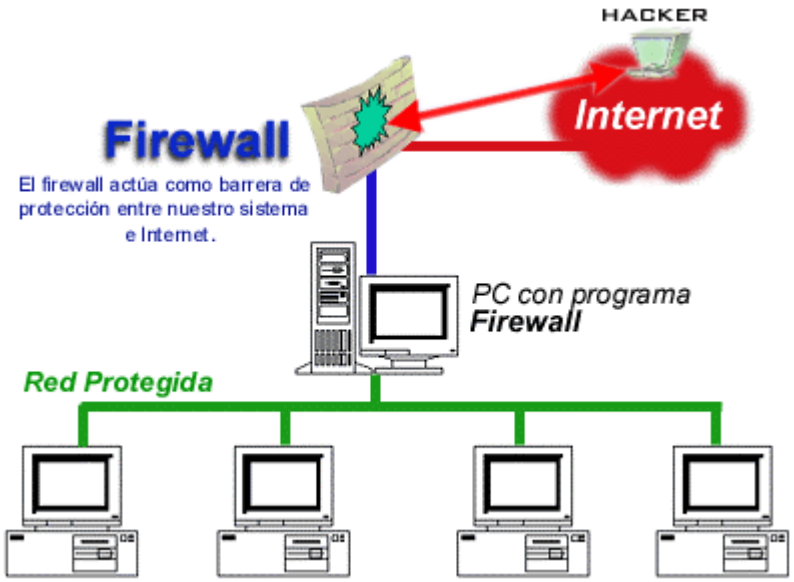
Apéndice C: Firewall

Conocimientos Previos

Para la confección del siguiente documento, se basó en la lectura de los puntos [1], [2] y [11] presentados en la Bibliografía.

Definición

Un Firewall es un sistema básico de seguridad, que instala una barrera entre cada computador de la red interna e Internet. Todo el tráfico de datos que circula desde y hacia Internet es autorizado o denegado por el Firewall, de acuerdo a la configuración que se le asigne. Si bien el Firewall acepta o deniega el tráfico, no sucede lo mismo con el contenido del mismo, por lo que se deberá instalar algún programa Antivirus que se encargue de esto.



El Firewall es un simple programa o dispositivo de hardware que filtra los paquetes de información proveniente de Internet, que entran a la red.

Como filtro de información usan uno de los siguientes métodos:

- Packet filtering: los paquetes son analizados según un conjunto de filtros, los cuales determinan que conjunto de paquetes pueden pasar y cuales no. Este tipo de Firewall es uno de los más rápidos porque no examina los datos del paquete. Básicamente examina en el paquete las direcciones IP de la fuente y del destino así como la combinación de puertos y aplica las reglas de filtrado.
- Proxy service: Este tipo de Firewall fuerza a todas las aplicaciones de clientes sobre las estaciones de trabajo protegidas por el Firewall, a pasar a través de él. El Firewall autoriza a cada uno de los paquetes por cada protocolo en forma diferente. El Firewall debe tener el servicio proxy corriendo en él por cada tipo de protocolo que pueda ser usado y todos los equipos de la red necesitarán que

se les instale el cliente proxy. Si bien son consideradas muy seguras, son en muchos casos muy lentas.

- Stateful inspection: En este Firewall, todas las conexiones son monitoreadas y sólo aquellas que son encontradas válidas son permitidas pasar a través del Firewall. Esto generalmente significa que el cliente detrás del Firewall pueden iniciar cualquier tipo de sesión, pero los clientes que están fuera del Firewall no pueden ver o conectarse a una máquina protegida por el Firewall.
- Firewall usando Network Address Translation (NAT) y/o Port Address Translation (PAT): ocultan completamente la red protegida por el Firewall. En muchas implementaciones hay una sola dirección IP pública usada por la red entera.

Algunos posibles filtros que se aplican son los siguientes:

- Direcciones IP o nombre de dominios: Si una dirección IP fuera de la empresa está leyendo demasiados archivos de un servidor, el Firewall puede bloquear todo el tráfico desde y hacia dicha dirección.
- Protocolos: Se pueden aplicar filtros sobre los siguientes protocolos:
  - IP (Internet Protocol)
  - TCP (Transport Control Protocol)
  - HTTP (Hyper Text Transfer Protocol) : páginas web.
  - FTP (File Transfer Protocol): usado para transferencia de archivos
  - UDP(User Datagram Protocol): usado para información que no requiere respuestas, como por ejemplo audio y video.
  - ICMP (Internet Control Message Protocol): utilizado por un router para intercambiar información con otros routers.
  - SMTP (Simple Mail Transport Protocol): utilizado para enviar información basada en texto, por ejemplo e-mails.
  - SNMP (Simple Network Management Protocol): usado para colectar información desde una computadora remota.
  - Telnet: usado para ejecutar comandos en una computadora remota.

Cuando conectamos nuestra red a Internet, los potenciales intrusos rastrean computadoras a través de este sistema buscando puertos que puedan allanar y entrar, para luego violar la seguridad.

Los objetivos de estos accesos indebidos son diversos. Entre los que más se destacan se encuentran:

- Login remoto: conexión remota hacia el computador intentando tomar el control en alguna forma, con la intención de acceder a los archivos o programas que están corriendo.
- Aplicaciones “backdoors”: Algunos programas poseen puertas traseras o backdoors que otorgan niveles de control a quien intenta acceder remotamente. Muchas veces los sistemos operativos tienen bugs que actúan como backdoors, vulnerabilidad que es usada por los hackers.
- SMTP session hijacking: SMTP es el método más común de envío de email en Internet. Obteniendo acceso a las listas de correo una persona puede producir correos spam a cientos de usuarios. Esto es realizado con frecuencia

redirigiendo los emails a través de un server SMTP de un host no conocido, haciendo que quién envía el spam sea difícil de detectar.

- Denial of service: El hacker envía una solicitud al servidor de conexión. Cuando el servidor responde intentando establecer una sesión, no puede encontrar a quién hizo la solicitud. Inundando al servidor con estas solicitudes, se logra bajar notablemente la performance del equipo e incluso, hasta es posible que el servidor se caiga.
- Envío masivo de emails: intentan que el sistema de email se sature enviando cientos de emails al mismo tiempo.
- Macros y virus: comando script y virus que pueden destruir los datos hasta producir una caída del sistema.
- Ruteo de la fuente: cambios en la información que circulan por la red, cambiando cabezales donde se indica por cuál router el paquete debe viajar. De esta forma paquetes dicen venir de fuentes en las cuales se confía y son aceptadas por el servidor.

Muchos de estos problemas son difíciles de detectar usando un Firewall. Es de suma importancia que se posea un sistema de Antivirus instalado en toda la red.

Se debe establecer en la configuración del Firewall, qué paquetes pueden pasar y cuáles no, para lo cual se debe conocer con exactitud la información que la empresa necesita determinando exactamente el tráfico que se debe producir a través del Firewall.

Tipos de Redes Firewall

Conceptualmente, existen dos tipos de Firewall:

- Nivel de red: el tráfico es examinado a nivel de paquete, en el protocolo de red.
- Nivel de aplicación: es un sistema en el que el servicio se proporciona por procesos que mantienen estados de conexión completos con TCP y secuenciamiento. A menudo redirigen el tráfico saliente, es como si se hubiera originado desde le Firewall y no desde el host interno.

Los **Firewalls a nivel de red** generalmente toman las decisiones basándose en la fuente, dirección de destino y puertos, todo ello en paquetes individuales IP. Un simple router es un "tradicional" Firewall a nivel de red. Los modernos Firewall se han sofisticado manteniendo información interna sobre el estado de las conexiones que están pasando a través de ellos, los contenidos de algunos datagramas y otras cosas.

Una característica importante es que enrutan el tráfico directamente a través de ellos, de forma que cada usuario necesita tener un IP asignado. Este tipo de Firewall tiende a ser más veloz y más transparente a los usuarios.

La idea principal de esta arquitectura es acceder a y desde un único host el cual es controlado por un único router operando a nivel de red.

Los **Firewalls a nivel de aplicación** son generalmente, host que corren bajo servidores proxy, que no permiten tráfico directo entre redes y que realizan login elaborados y auditan el tráfico

que pasa a través de ellas. Las Firewall a nivel de aplicación se puede usar como traductoras de direcciones de red, desde que el tráfico entra por un extremo hasta que sale por el otro.
Tienden a proporcionar mayor detalle en los informes auditados e implementan modelos de conservación de la seguridad.

Cada vez más, los firewalls incorporan encriptación, protegiendo así el tráfico que se produce entre ellos e Internet. Los firewalls con mecanismos de encriptación end to end, se pueden utilizar para organizaciones con múltiples puntos de conexión a Internet, utilizándola como una "red privada"donde no sea necesario preocuparse de que los datos o contraseñas puedan ser capturadas.

Cómo hacer para que trabajen Web / Http con una Firewall.

Hay tres formas de conseguirlo:

- Permitir establecer conexiones vía un router, si se están usando routers protegidos
- Usar un cliente Web que soporte SOCKS, y correr SOCKS en tu Firewall.
- Ejecutar alguna clase de servidor Web Proxy en la Firewall, el cual podría incluir Proxy Web, Gopher y FTP.

Cómo hacer para que trabaje FTP a través de un Firewall

Generalmente se consigue usando un servidor Proxy FTP o bien realizando alguna de las dos opciones siguientes:

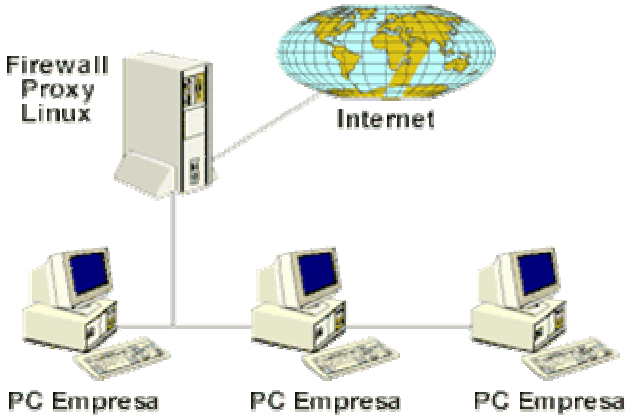
- Permitiendo conexiones entrantes a la red en un rango de puerto restringido.
- Restringiendo las conexiones entrantes usando alguna clase de reglas de protección preestablecidas.

Instalación de Firewall

Cuando se instala un Firewall, la conexión a Internet debe estar realizada, pero no tiene que estar conectada a la red protegida.

Al instalar el Firewall, se deben testear las funciones básicas del equipo para luego comenzar con la configuración detallada del firewall previo ciertas reglas determinadas con anticipación. Son aspectos fundamentales en la configuración del Firewall saber con anterioridad la política de acceso que se pondrá en práctica, configuraciones para correo electrónico, dónde se ubicará la información de login, etc.
Cuando ya se tienes todos los aspectos de configuración del Firewall debidamente determinados, se procede a la configuración del mismo, luego se conecta a Intenet y se testea que las operaciones de red sean correctas. Es en este momento cuando se instalan y chequean las reglas para el control de acceso al firewall y se conectan a la red protegida. También se deben realizar el control de funcionamiento de los accesos a Web, correo electrónico, etc.

Ejemplo de Firewall: Firewall Linux



Una solución de seguridad muy económica y altamente confiable, es la habilitación de un servidor dedicado operando bajo plataforma **Linux**, el cual se instala y configura adecuadamente para funcionar como un robusto Firewall. Entre los servicios que se habilitan en el servidor, se destacan:

- Servidor Proxy HTTP y FTP con Cache de disco para acelerar la navegación por Internet.
- Informes generadores de forma automática que permiten ver y evaluar el uso que se le está dando a Internet al iterior de la empresa. Podrá controlar por donde navegan los usuarios.
- Conversión de las direcciones IP de su red privada (NAT)
- Servicios HTTP, FTP y Correo.
- Servicio de WebMail.
- Servidor DNS.

Servidores Proxy y su funcionamiento

Un servidor Proxy es una aplicación que media en el tráfico que se produce entre una red protegida e Internet. Los Proxies se utilizan a menudo, como sustitutos de routers controladores de tráfico, para prevenir el tráfico que pasa directamente entre las redes.

Muchos Proxies contienen login auxiliares y soportan la autentificación de usuarios. Un Proxy debe entender el protocolo de la aplicación que está siendo usada, aunque también pueden implementar protocolos específicos de seguridad (por ejemplo: un proxy FTP puede ser configurado para permitir FTP entrante y bloquear FTP saliente).

Los servidores Proxies son aplicaciones específicas. Tenemos Proxies para Telnet, FTP, http/Web, etc. SOCKS es un sistema Proxy genérico que puede ser compilado en una aplicación cliente para hacerla trabajar a través de un Firewall.

Una función que es frecuentemente combinada con un Firewall es un Proxy Server. Un Proxy Server es una aplicación de gateway que corre por encima de un sistema de propósito general tal como UNIT o NT. Estos gateways operan en la capa más lata del modelo OSI, la capa 7, la

cual les permite mantener estado de sesión y soportar autentificación de usuario, manteniendo la seguridad.

Con un Proxy Server, los usuarios ganan acceso a la red pero a través de procesos que establecen el estado de la sesión, autentificación de usuario y políticas de autorización. El Proxy Server ofrece seguridad porque la sesión es retenida en la capa de aplicación.

Se debe tener en cuenta que este tipo de seguridad posee un gran costo en performance, siendo intensivo el proceso de operaciones que consumen muchos ciclos de CPU, limitando así el número de sesiones en tiempo real.

El Proxy Server es usado para acceder a páginas Web por las computadoras de la red interna.. Cuando una computadora solicita una página web, esta es solicitada por el Proxy Server y luego enviada a quien la solicitó. El efecto que esto produce es que las computadoras remotas solicitando la página Web nunca acceden a nuestra red, sino que lo hacen solamente con el Proxy Server.

Ofrecen también eficiencia en los accesos hacia Internet. Todas las páginas accedidas desde la red, son almacenadas en Caches en el Proxy Server, de forma tal que la próxima vez que éstas sean solicitadas, no necesitará cargarlas nuevamente de Internet, tomándolas de su Cache.

Existe la posibilidad de que usuarios remotos necesiten acceder a ciertos servicios que corren sobre la red, como pueden ser Web Site, aplicaciones online o download y upload FTP. En estos casos, se debe crear una zona desmilitarizada (DMZ). (Ver Apéndice C.)

Apéndice D - Zona Desmilitarizada (DMZ)

Consideraciones Generales

Para la confección del siguiente documento, se basó en la lectura de los puntos [3] y [4] presentados en la Bibliografía.

Definición

DMZ es una línea de frontera que protege la información de la red interna, hacia Internet. DMZ separa una red externa (Internet) de una red interna (red empresarial), aislando la máquina que está directamente accedida desde todas las máquinas de la red. Comúnmente, la máquina que se aísla dentro del DMZ es el Web Server.

La idea fundamental, entonces es el de proteger la información de valor que se encuentra en la red interna, de posibles ataques que se susciten desde Internet, los cuales pueden llegar a alcanzar todo el sistema. Se debe diseñar el DMZ de forma de que los ataques, si alcanzan el Web Server no pueda pasar a través de él y no alcance la base de datos empresarial. Este es el problema fundamental que intenta resolver el DMZ.
En casos en que se desee que usuarios remotos tengan acceso a la red a través de un Web Site o un área FTP (download y upload), entonces se deberá crear una zona desmilitarizada (DMZ).

Diseño del DMZ

Usualmente, la puerta de entrada al sistema es el Web Server, que como se mencionó anteriormente, se ubica dentro del DMZ.

Un Firewall frecuentemente protegería a una DMZ de amenazas externas. Como el servidor debe comunicarse hacia el exterior (Internet), el Firewall debe ser configurado para la administración de cierto tipo de conexiones de red, protegiendo el/los servidor/es que se encuentra (/n) en el DMZ.

Entonces, el Web Server debe tener una tarjeta de hacia el Firewall. Otra posible configuración, que no tiene porqué ser la más segura configuración, es colocar en el Web Server dos tarjetas de red. Una de las tarjetas que maneje el tráfico saliente del Firewall hacia el Web Server y la otra el tráfico entrante. Esto ofrece más protección respecto a tener una sola tarjeta de red, en términos de la capa física del modelo OSI, en lo que a posibles ataques se refiere.

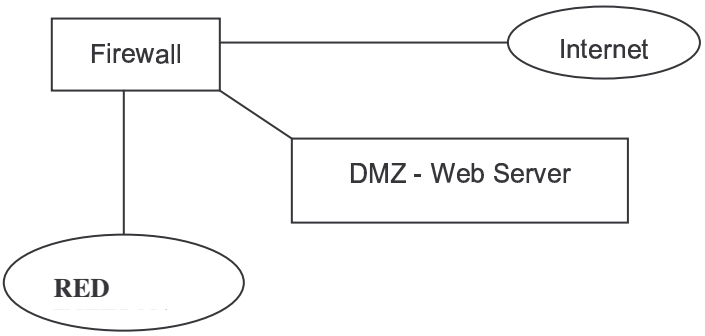
Otra configuración que se debe tener en cuenta, es la de configurar el Web Server (equipo dentro del DMZ) con un conjunto de usuarios y passwords completamente diferentes a la de la red interna. De este modo, si el DMZ es atacado, se mantienen protegidas las máquinas de la red interna.

La más segura configuración de red para un DMZ es separar la red externa, la zona desmilitarizada y la red interna, ubicándolas en diferentes subredes, permitiendo así que el

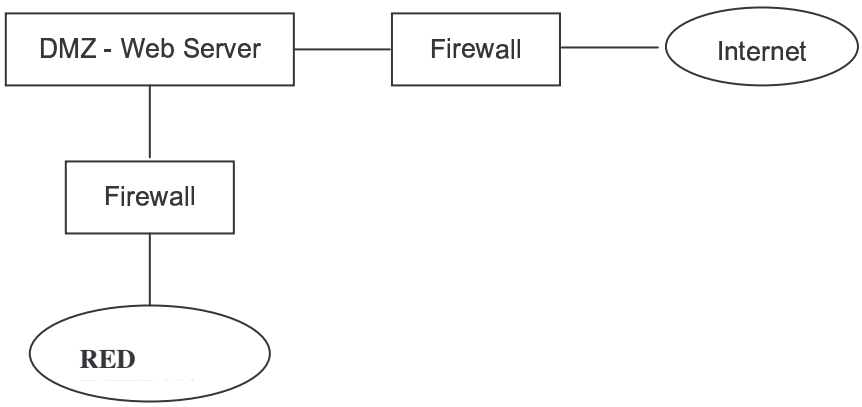
tráfico de la red no pueda traspasar a las diferentes subredes sin ser ruteado, controlando que puede entrar o salir del DMZ. Los ataques, entonces tendrán solamente acceso a la máquina que se encuentra dentro del DMZ y no a todas la que se encuentran fuera de él.

Configuración de Firewall y DMZ

Se pueden usar uno o dos Firewall para crear un DMZ, pero se debe destacar que con el uso de dos Firewalls se logra más seguridad y confiabilidad en su diseño.



Configuración con un solo Firewall.



Configuración con dos Firewalls.

En esta configuración, usando dos Firewalls, se coloca un Firewall entre el Web Server (DMZ) e Internet y el otro entre la Red Interna y el Web Server. El primer Firewall debe permitir el pasaje del mínimo tráfico que se desea desde y hacia Internet. Se debe observar que se deben estudiar detenidamente las reglas que se aplicarán a cada unos de los Firewalls, dependiendo del tipo de acceso que se necesita, de acuerdo a las aplicaciones que se deben correr hacia y desde Internet.

Para ambas configuraciones, se puede configurar el DMZ teniendo una o dos tarjetas de red, tal como se menciona diseño del DMZ, mencionado anteriormente en el presente documento. Para obtener mayor seguridad y confiabilidad, lo ideal sería trabajar con dos tarjetas de red.

Apéndice E- Redes Privadas Virtuales

Consideraciones

Para la confección del siguiente documento, se tomaron como base la información obtenida en los puntos [5], [6], [7], [8], [9], [10], y [11] de la Bibliografía.

Definición

Una Red Privad Virtual (Virtual Private Network) proporciona un sistema de conectividad a redes que se encuentran a grandes distancias físicas. Esta conectividad se realiza utilizando otra red privada ya existente, como puede ser Internet, basándose en la idea de crear *túneles* (***tunneling***). Esta tecnología consiste en establecer y construir una conexión lógica de red, el túnel, sobre la cual los paquetes son encapsulados y transmitidos hacia su punto de destino.

En las VPNs basadas en Internet, los paquetes en un determinado protocolo VPN son encapsulados dentro de paquetes IP, y luego son enviados a través de esta red.

Los protocolos VPN deben soportar autentificación y encriptación para mantener túneles seguros.

Las Redes Privadas Virtuales se crean con la intención de conectar usuarios remotos a su red corporativa de forma segura, conectar oficinas distantes mediante túneles sobre Internet (extender la red corporativa o simplemente conectar oficinas entre sí),

Tipos de VPN

Existen dos tipos de túneles:

- voluntary tunneling: el cliente VPN maneja la conexión. El cliente primero hace la conexión con el proveedor de servicio de conexión (por ejemplo ISP = Internet Server Provider, en el caso de Internet). Luego la aplicación cliente VPN crea un túnel hacia el VPN server sobre la conexión de Internet.
- compulsory tunneling: El proveedor de servicio conexión maneja la conexión (por ejemplo el ISP). Cuando el cliente hace una conexión a su proveedor de servicio, inmediatamente, el proveedor crea una conexión entre el cliente y el servidor VPN.

Protocolos de VPN

Existen tres diferentes protocolos VPN especialmente diseñados para el uso de túneles VPN, siendo incompatibles unos con otros:

- Point to Point Tunneling Protocol (PPTP)
  Es un protocolo de túneles que provee el acceso mediante múltiples protocolos a una red, sobre Internet. Protocolos de capa de red como IPX y NETBEUI son encapsulados por el protocolo PPTP sobre Internet.
  PPTP es construido por Microsoft e incluido en su versión NT 4.0. Se ha detectado que posee es sensible a ataques y no permite más de 255 conexiones concurrentes por servidor. Asimismo permite que un cliente mantenga un solo túnel con el servidor. Por otro lado, presenta bajo costo de integración con Windows 3.11, 95 y 98.
  Como PPTP fue creado sobre la base de la conexión dial up, soporta una variedad de configuraciones de red: líneas telefónicas, ISDN, framerelay y x.25.

- Layer Two Tunneling Protocol (L2TP)
  Es el sucesor del protocolo PPTP, que surge de la combinación de PPTP y otro protocolo L2F (protocolo implementado en productos Cisco). Permite la conexión múltiple y simultánea de túneles para cada usuario. Fue incorporado a Windows 2000.
  Puede crear túneles entre: Cliente y router, NAS y router, router y router.
  Trabaja en la capa 2 del modelo OSI.

- Internet Protocol Security (IPSec)
  Es una colección de múltiples protocolos relacionados. Puede ser usado como una completa solución VPN o puede ser usado como un esquema de encriptación dentro de L2TP o PPTP.
  Este protocolo provee mejores algoritmos de encriptación y autentificación suministrando chequeos de integridad de los datos transmitidos.
  IPSec puede encriptar datos entre varios dispositivos como ser: router a router, Firewall a router, Pc a router y PC a server.
  IPsec trabaja en la capa de red en el modelo OSI.

Tecnologías VPN

Dependiendo del tipo de VPN que se desee configurar, se deberán tener en cuentas las siguientes componentes, a la hora de construir una VPN:

- software cliente VPN en cada uno de los clientes
- Un Firewall o un concentrador VPN dedicado
- Un Servidor VPN dedicado a conexiones dial-up
- NAS (Network Access Server) usado por el proveedor de servicios para el acceso de los usuarios VPN.
- Red VPN y políticas de gerenciamiento.

Algunas soluciones de mercado, son las siguientes:

- Cisco VPN 3000 Concentrator: ofrece módulos para cada necesidad, pudiendo abarcar desde 100 usuarios remotos hasta más de 10.000 en forma simultánea
- Cisco 1750 Modular Access Router: Es un router optimizado.
- Cisco PIX Firewall: Combina NAT dinámicas, proxy server , filtro de paquetes y firewall, así como las capacidades de VPN en un solo elemento de hardware.

Bibliografía

[1] Jeff Tyson.
How Firewall Works.doc
http://computer.howstuffworks.com/firewall.htm

[2] José Ramón Esteban Martí.
Firewall-Cortafuegos
http://seguridad.internautas.org/firewall.php

[3] Liza Yeo. Junio 6, 2003.Prentice Hall
Chossing a Personal Firewall.
http://www.informit.com/articles/article.asp?p=31945

[4] Scott Young, "Designing a DMZ". Assignment Version 1.2b. March 26, 2001
www.giac.org/practical/gsec/Scot_Young_Gsec.pdf

[5] Introduction to VPN
http://compnetworking.about.com/library/weekly/aa010701a.htm

[6] Christopher McDonald, AMS Center for Advanced Technologies (AMSCAT)
Virtual Private Networks. An overview.
http://www.intranetjournal.com/text/foundation/vpn-1.shtml

[7] Jeff Tyson.
How Virtual Private Networks Works
http://computer.howstuffworks.com/vpn.htm

[8] La Administración de Redes Virtuales con PPTP
Windows NT Magazine. Número 29 - Marzo'99
http://www.windowstimag.com/atrasados/1999/29_mar99/articulos/internet.htm

[9] Microsoft Corporation. Last Updated: Wednesday, June 27, 2001
What is PPTP
http://www.microsoft.com/ntserver/ProductInfo/faqs/PPTPfaq.asp

[10] Microsoft Windows 2000 Professional vpn.doc
Microsoft Windows 2000 Professional Documentation

[11] Firewall y Redes Privadas Virtuales
www.softdownload.com.ar

[12] Pawel Skonecki, v2.1a, 2001-10-06
http://ldp.kernelnotes.de/HOWTO/Call-back.html