

14
24



UNIVERSIDAD NACIONAL AUTONOMA
DE MEXICO

FACULTAD DE INGENIERIA

AUDITORIA A LA RED DE TELECOMUNICACIONES
DE UNA SOCIEDAD NACIONAL DE CREDITO

T E S I S

QUE PARA OBTENER EL TITULO DE
INGENIERO EN COMPUTACION
P R E S E N T A N :
ANA ROSA CANTON GARCIA
ALEJANDRO M. CORREA HERNANDEZ

DIRECTORES DE TESIS

ING. JOSE DIAZ BARRIGA SILVA

ING. ALBERTO TEMPLOS CARBAJAL



MEXICO, D. F.

TESIS CON
FALLA DE ORIGEN

1991



UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

DERECHOS RESERVADOS © PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis está protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

14
24

UNIVERSIDAD NACIONAL AUTONOMA
DE MEXICO

FACULTAD DE INGENIERIA



AUDITORIA A LA RED DE TELECOMUNICACIONES
DE UNA SOCIEDAD NACIONAL DE CREDITO

T E S I S

QUE PARA OBTENER EL TITULO DE
INGENIERO EN COMPUTACION
P R E S E N T A N :
ANA ROSA CANTON GARCIA
ALEJANDRO M. CORREA HERNANDEZ

DIRECTORES DE TESIS

ING. JOSE DIAZ BARRIGA SILVA

ING. ALBERTO TEMPLOS CARBAJAL



MEXICO, D. F.

TESIS CON
FALLA DE ORIGEN

1991

CONTENIDO

	Introducción	I
I	CONCEPTOS NECESARIOS DE AUDITORIA, COMUNICACIONES Y BANCA	1
1.1	Conceptos De Auditoría	3
1.1.1	Auditoría Tradicional	3
	Definición	3
	Necesidad	4
1.1.2	Requisitos y Cualidades del Auditor Tradicional	4
1.1.3	Tipos de Auditores	4
	Auditores Independientes	4
	Auditores Internos	4
	Auditores de Interés Especial	5
	El Auditor Como Técnico Experto	5
	El Auditor de Sistemas	5
	Especialista en Auditoría de Proceso Electrónico de datos (PED)	7
	Supervisor de Auditoría de PED	7
1.1.4	Características del Auditor de PED	7
	Responsabilidades	7
	Deberes	7
	Experiencia Requerida	8
1.1.5	Objetivos de la Auditoría de PED	9
1.1.6	Planeación de Auditoría	12

	Fases de la Planeación de Auditoría	12
1.2	Conceptos de Telecomunicaciones	13
1.2.1	Antecedentes Históricos	13
1.2.2	Definiciones Básicas	16
	Tipos de Procesamiento	16
	Tipos de Modulación de Señal	23
	Baudio (Baud)	24
	Velocidad en Baudios (Baud Rate)	24
	Capacidad de un Canal de Comunicaciones	24
	Clasificación de Circuitos	25
	Circuitos y Modos de Operación	25
	Líneas Privadas (Dedicadas) y Conmutadas	27
	Banda de Paso	27
	Ancho de Banda	28
	Sondeo(Polling)	28
1.2.3	Estructuras de las Redes	31
1.3	Antecedentes de la Banca	35
1.3.1	Antecedentes Históricos de la Banca	35
	Banca Comercial	35
	Banca de Inversión	35
	Multibanca	35
	Aspectos Importantes del Sistema Financiero Mexicano	35
1.3.2	Estructura Bancaria Nacional Actual	36
	Reordenación del Sistema Bancario	36

1.3.3	El Sistema Financiero Mexicano	37
	Secretaría de Hacienda y Crédito Público	37
	Comisión Nacional Bancaria y de Seguros	37
	Banco de México	38
	Sociedades Nacionales de Crédito	38
	Organizaciones Auxiliares de Crédito	38
	Instituciones de Seguros	40
	Mercado de Valores	40
II	APLICACIONES Y COMPONENTES PRINCIPALES DE LA RED DE TELECOMUNICACIONES	41
2.1	Alcance de la Auditoría	43
2.2	Definir Base Instalada	44
2.3	Técnicas de Auditoría	45
III	SEGURIDAD DE LA RED	47
3.1	Definición de Sistema Seguro	49
3.2	Requerimientos de Seguridad	50
3.3	Características de Seguridad Relacionadas con el Mensaje	52
3.4	Recuperación de una Falla del Sistema	54
3.5	Requerimientos Operacionales para la Seguridad y Confiabilidad	54

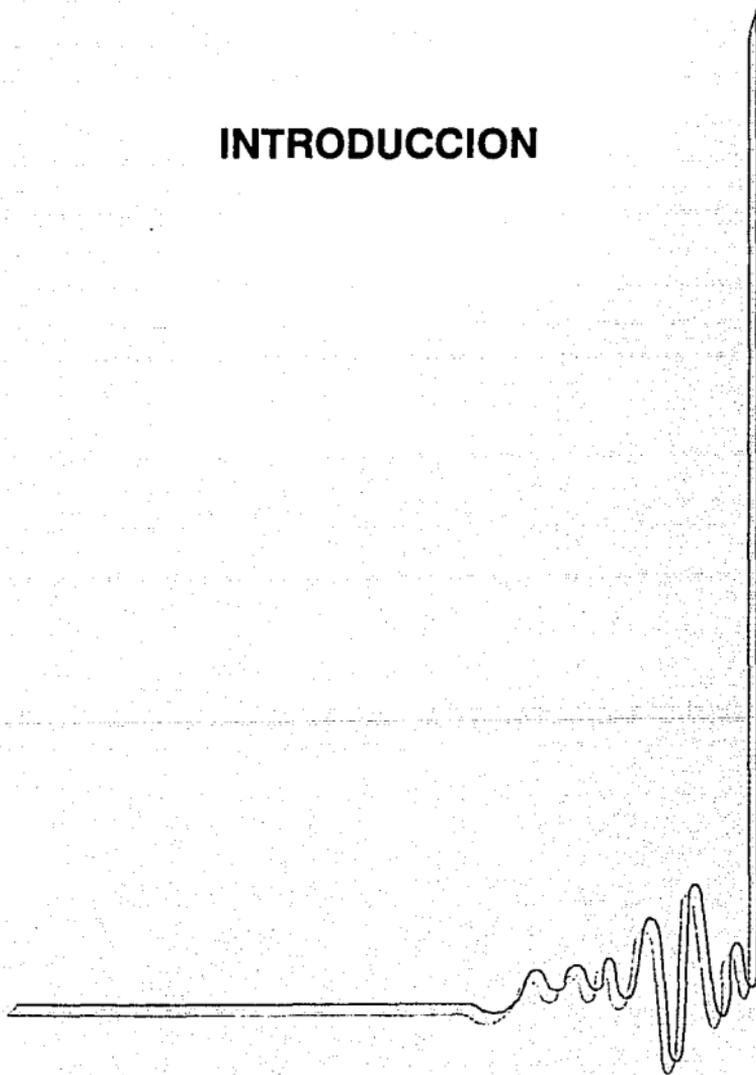
3.6	Definición de un Sistema de Telecomunicaciones Seguro	56
3.6.1	Seguridad Administrativa	56
3.6.2	Seguridad en Software	57
3.6.3	Seguridad en Hardware	58
3.6.4	Planes de Contingencia	59
3.6.5	Seguridad Física	61
3.6.6	Seguridad en la Transmisión	64
IV	DESEMPEÑO Y EFICIENCIA DE LA RED	65
4.1	Conceptos Básicos de Muestreo	67
4.2	Métodos de Muestreo	68
4.3	Aspectos a Evaluar del Desempeño	68
4.4	Aspectos a Evaluar de la Eficiencia	71
V	ADMINISTRACION DE LA RED	73
5.1	Aspectos a Evaluar de la Administración de la Red	76
5.2	Evaluación de Requerimientos Futuros	81

VI	INFORME DE AUDITORIA	83
6.1	Elementos Básicos del Informe	85
6.2	Características de un Informe	86
6.3	Discusión de las Conclusiones y Recomendaciones con los Responsables de las reas Auditadas	87
6.4	Seguimiento de las Observaciones del Informe	87
VII	CASO PRACTICO	89
	Alcance de la Auditoría	89
	Definir Base Instalada	90
	Servicios que Ofrecen las Sociedades Nacionales de Crédito	90
	Base Instalada	95
	Seguridad de la Red	110
	Seguridad Administrativa de la Red	110
	Software para la Seguridad de la Red	110
	Hardware para la Seguridad de la Red	111
	Planes de Contingencia	116
	Seguridad Física	120
	Controles de Fuego	120
	Controles de Agua	121
	Controles de Electricidad	121
	Controles de Acceso	122
	Controles de Aseo y Mantenimiento	122
	Controles de Asuntos Generales	122

Seguridad de Transmisión	123
Synchronous Data Link Control (SDLC)	128
Estándar X.25	128
Desempeño	131
Eficiencia	148
Evaluación de la Administración	152
Evaluación de Requerimientos Futuros	158
Informe de Auditoría	160
CONCLUSIONES	167
ANEXO I SERVICIOS QUE OFRECEN LAS SOCIEDADES NACIONALES DE CREDITO	171
Captación de Recursos	173
Créditos Bancarios	174
Servicios Nacionales e Internacionales	175
Servicios Relacionados con Valores	176
Servicios Relacionados con Fiduciario	177
Otros Servicios	177

ANEXO II	DESCRIPCION DE LOS EQUIPOS DE LA RED	179
	Unisys 2200/400	181
	Sistema 38 de IBM	191
	SNA	194
ANEXO III	TIPOS DE MUESTREO	199
	Muestreo de Criterio	201
	Muestreo Estadístico	202
	Muestreo de Atributos	204
	Muestreo de Variables	205
CUADRO A		211
CUADRO B		231
Bibliografía		

INTRODUCCION



INTRODUCCION

La operación diaria de cualquier empresa es en gran medida dependiente de la comunicación de datos, por lo que es de suma importancia tener atención especial a la red de telecomunicaciones.

En una red de telecomunicaciones es esencial que las partes involucradas confíen en la validez y oportunidad de los datos. Para poder garantizarlo, es importante que una persona independiente pueda examinarla con el fin de emitir una opinión profesional sobre el estado de ésta. Desafortunadamente, la gente considera al auditor como el "hombre que dispara a los heridos después de la batalla", mientras que las tendencias actuales de auditoría es hacer su función como un mantenimiento preventivo en el análisis y evaluación de la confiabilidad e integridad de los sistemas de procesamiento y transferencia de datos.

Como la auditoría en esta área es una disciplina relativamente nueva, hay pocas descripciones de cargos que sean de aceptación general. Juzgar a un candidato para desarrollar la auditoría basándose en un conjunto de criterios e impresiones generales en lugar de usar criterios formales, puede resultar injusto tanto para el candidato como para la organización, por lo que se deben establecer metas realistas y tanto el auditor como la empresa deben saber lo que esperan el uno del otro.

El auditor debe considerar que los sistemas en proceso distribuido no sólo asignan el procesamiento en sitios múltiples, sino también los activos de la empresa. Esta configuración junto con controles inadecuados brinda una oportunidad para cometer fraudes. En muchas ocasiones se ha observado que el período perfecto para un fraude es anterior a la implementación de controles.

Con el incremento de fraudes relacionados con el equipo de cómputo, muchas empresas acuden a los auditores para no verse involucradas en estas situaciones, por lo cual las empresas han llegado a comprender la importancia de la función de auditoría y a tomar en cuenta los resultados de las mismas.

La necesidad de poner a funcionar los sistemas a tiempo y dentro del presupuesto ha limitado el que se haga énfasis en el control, por lo cual se han desperdiciado muchos recursos al implantar proyectos que no son seguros, por lo cual es importante que un auditor se integre al equipo de desarrollo. Esto representa un costo extra pero nos garantiza la calidad del producto y un ahorro en los resultados finales.

La rápida multiplicación de los dispositivos terminales y el crecimiento de los sistemas distribuidos son un reto para tener un sistema seguro. Aunque no existe un sistema perfecto de comunicaciones de datos, hay varios conceptos y requerimientos de diseño que los auditores deberían comprender para simplificar sus evaluaciones y para permitirles someter recomendaciones razonables.

En esta tesis no pretendemos dar una solución de "receta de cocina" a todos los problemas, ya que simplemente no existen soluciones estándar, realmente la enfocamos como una metodología general para auditar cualquier red de telecomunicaciones.

A lo largo de la tesis manejamos diversas preguntas las cuales es indispensable que el auditor pueda responder para tener los elementos necesarios con objeto de determinar la situación de cada uno de los aspectos que se evalúan.

En un principio se revisan una serie de conceptos de auditoría, comunicaciones y banca para poseer un conocimiento estándar de estos.

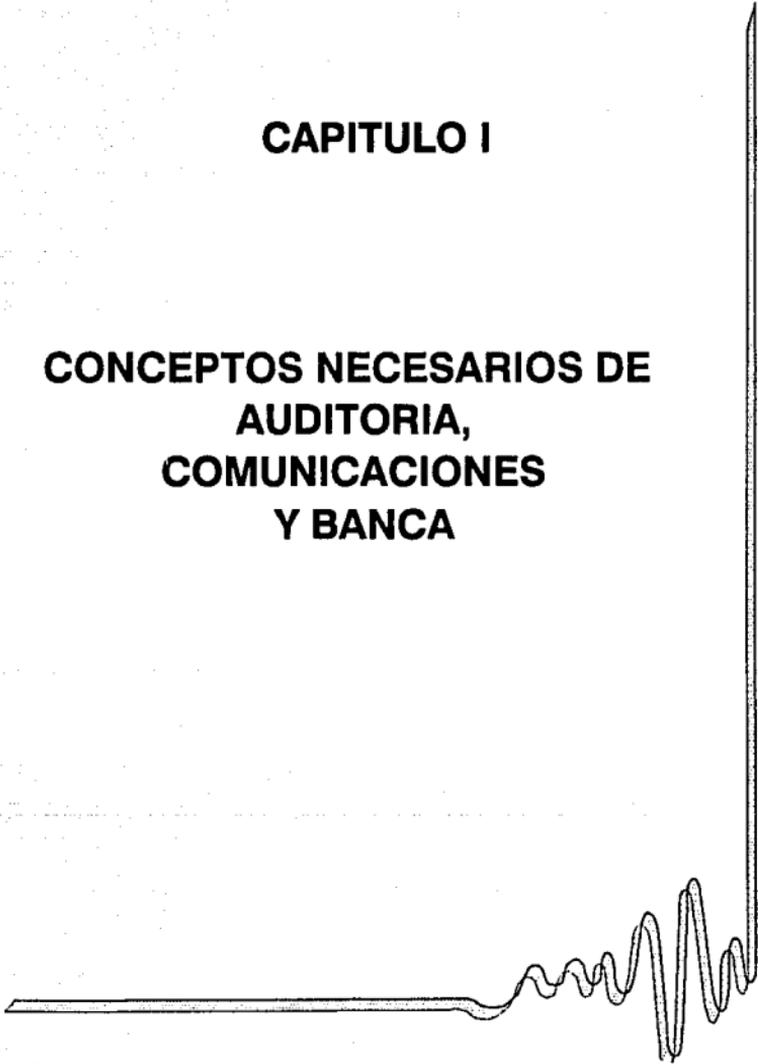
El primer capítulo de la tesis lo dedicamos a definir una serie de conceptos de las tres áreas involucradas: auditoría, comunicaciones y banca. En el segundo se define el alcance de la auditoría y se describen los lineamientos para obtener los elementos que componen la red a analizar (base instalada), utilizando las técnicas de auditoría, ya que conocemos el alcance y tenemos una visión de la red, en el siguiente capítulo se analiza uno de los puntos de mayor relevancia en una auditoría, la seguridad. No es suficiente el tener un sistema seguro, también se debe garantizar el buen desempeño y eficiencia de la red que se analiza en el cuarto capítulo, el último aspecto que se cubre es el de administración de la red, de la que dependen todos los puntos anteriores, a su vez se evalúan los requerimientos futuros para que sean acordes a los avances tecnológicos.

Una vez concluida la auditoría, en el sexto capítulo se mencionaran las características y elementos del informe de auditoría, así como la discusión de la misma con los usuarios.

El séptimo capítulo es un caso práctico donde se observa la aplicación de la metodología antes descrita.

CAPITULO I

CONCEPTOS NECESARIOS DE AUDITORIA, COMUNICACIONES Y BANCA



CAPITULO I

CONCEPTOS NECESARIOS DE AUDITORIA, COMUNICACIONES Y BANCA

Antes de empezar a desarrollar la auditoría de telecomunicaciones, es necesario conocer una serie de conceptos relacionados con nuestro tema de estudio.

De tal manera que el objetivo de este capítulo es presentar en forma sencilla los conceptos necesarios para poder entender los tres puntos básicos de estudio :

Auditoría
Comunicaciones
Banca

Es importante tener una idea clara de estos temas, para poder relacionarlos entre sí, ya que no es suficiente conocerlos en forma aislada.

1.1. CONCEPTOS DE AUDITORIA

En este subcapítulo se definen una serie de conceptos para ayudarnos a comprender qué es la auditoría, cuál es el papel del auditor y su aplicación en el proceso electrónico de datos (PED).

Debido a que con frecuencia el término de "auditoría" es ubicado en el área contable (estados financieros), presentaremos las características principales del auditor y auditoría tradicional así como la transición a una serie de áreas que en la actualidad se han cubierto (auditorías de interés especial).

1.1.1. AUDITORIA TRADICIONAL

Definición

Auditoría es la actividad por la cual se verifica la corrección contable de las cifras de los estados financieros; es la revisión misma de los registros y fuentes de contabilidad para determinar la razonabilidad de las cifras que muestran los estados financieros emanados de ellos.

Necesidad

La necesidad del examen de estados financieros es indiscutible; el administrador y el inversionista lo necesitan como un elemento importante para toma de decisiones, en primer lugar, para conocer la situación financiera de la empresa que administra o en la que desea invertir, y segundo, para tener la certeza de que tal situación financiera corresponde a la realidad que vive el negocio.

1.1.2. REQUISITOS Y CUALIDADES DEL AUDITOR TRADICIONAL

El contador público es un profesionalista y como tal, poseedor de un grado superior de habilidad en la técnica contable; habilidad desarrollada con el estudio, la práctica y las características personales. Como todos los profesionistas, el contador público debe reunir ciertos atributos de carácter personal y técnico que lo capaciten técnicamente en el ejercicio de su profesión.

1.1.3. TIPOS DE AUDITORES

Auditores Independientes

El trabajo del auditor independiente es, el de expresar una opinión sobre la honradez, con la cual los estados financieros presentan la posición financiera y sus cambios, y los resultados de las operaciones de la empresa bajo estudio. En el informe, el auditor declara si su investigación ha sido llevada al cabo de acuerdo con las normas de auditoría generalmente aceptadas.

Auditores Internos

La auditoría interna es una evaluación independiente de operaciones dentro de una empresa. Es una función de control administrativo que mide y valora la eficacia de otros controles.

El objetivo de la auditoría es ayudar a todos los miembros de la administración en el cumplimiento eficaz de sus responsabilidades.

Auditores de Interés Especial

El auditor es un agente contratado que brinda una opinión profesional sobre la confiabilidad de la posición financiera informada de una empresa. El auditor interno es un empleado de la entidad para la cual se expiden los informes de auditoría. Por otra parte los auditores de interés especial normalmente trabajan ya sea para un organismo gubernamental o para una empresa que hace negocios con el grupo objeto de revisión contable.

El Auditor Como Técnico Experto

Los métodos tradicionales para hacer auditoría "alrededor de la computadora" se están tornando obsoletos rápidamente a causa de las tendencias tecnológicas que hacen a las operaciones y a los datos "invisibles".

Además, el procesamiento electrónico de información introduce muchos riesgos nuevos. La concentración de información que resulta de la tecnología hace surgir problemas tales como contingencia, reconstrucción de datos, seguridad física y robo de servicios y datos.

Todos estos resultados exigen que el auditor se "asocie con la computadora". Para hacer esto eficazmente, el auditor debe tener conocimientos de lenguajes de programación, operaciones con la computadora, hardware, software, y análisis de sistemas, ser capaz de preparar programas o de utilizar paquetes de software de auditoría para evaluar la operación de un sistema.

El Auditor de Sistemas

Es recomendable que el auditor de sistemas tenga experiencia en auditoría y ser conocedor tanto en áreas funcionales como en seguridad de centros de procesamiento de datos y en auditoría de aplicaciones, ya que el auditor de sistemas, está involucrado en el esfuerzo de programación. Este miembro del personal debe tener excelentes aptitudes de comunicación y estar familiarizado con los paquetes de software de auditoría que se utilizan.

El auditor de sistemas debe tomar en cuenta :

- 1) Que el riesgo, no significa simplemente considerarlo como parte de la revisión de un sistema o de la auditoría de alguna función de proceso de datos. EL riesgo siempre debe ser una primera preocupación del auditor y gobernar no solo lo que haga sino cuando lo haga. El auditor además de reconocer problemas debe convencer y alentar a la administración a tomar la acción correctiva oportuna.
- 2) Una pista de auditoría adecuada de modo que las transacciones puedan rastrearse hacia adelante y atrás de un sistema.
- 3) Los controles contables de toda entrada y los controles para garantizar la integridad de aquellas transacciones a lo largo del segmento mecanizado del sistema.
- 4) El manejo de excepciones y rechazos del sistema de cómputo.
- 5) La prueba para cerciorarse si los sistemas funcionan tal y como se declaró.
- 6) El control sobre cambios del sistema de cómputo, con el objeto de determinar si se ha dado la autorización correcta.
- 7) Los procedimientos de autorizaciones para eliminaciones del sistema.
- 8) Determinar si se ha incluido la adhesión a las políticas y procedimientos tanto gubernamentales como de la empresa en la implantación del sistema.
- 9) Vigilar la capacitación del personal usuario en la operación del sistema.
- 10) Desarrollar criterios detallados de evaluación para que sea posible determinar si el sistema implantado ha cumplido satisfactoriamente con las especificaciones predeterminadas.
- 11) Los controles adecuados entre computadoras interconectadas.
- 12) Los procedimientos de seguridad adecuados para proteger los datos del usuario.

Especialista en Auditoría de PED

Tiene suficiente experiencia como para evaluar el rendimiento de una aplicación, por lo general tiene conocimientos semejantes al de un analista de sistemas, puede analizar sistemas en operación y hacer comentarios sobre la suficiencia de los controles y cuáles aspectos de controles deben implementarse.

Supervisor de Auditoría de PED

Mediante el desarrollo de procedimientos para la auditoría de sistemas y el uso de la computadora para las auditorías periódicas, desarrolla estándares y pautas de control para sistemas y actúa como fuente central de conocimientos técnicos de auditoría de PED para todos los auditores internos.

1.1.4. CARACTERÍSTICAS DEL AUDITOR DE PED

Responsabilidades

Responsable de una variedad de funciones de análisis, auditoría y procesamiento de datos diseñado para asegurar el mantenimiento de un control adecuado de los activos y de los registros financieros. Deberá mantener contacto personal periódico con los varios niveles del personal, además de comunicaciones continuas de tipo verbal y escrito. Puede asignarse la responsabilidad de supervisión de uno o más auditores en el desempeño de una misión, además deberá haber completado con éxito el estudio formal y el entrenamiento en disciplinas como contabilidad, auditoría, análisis de operaciones, administración, estadística, derecho mercantil y ciencias de la computación y ser capaz de aplicar esa educación en su trabajo.

Deberes

Actuará como consultor e instructor en diseños de sistemas de cómputo mediante su participación como miembro del grupo de desarrollo de sistemas. En tal capacidad revisará los controles, la retención de registros, la documentación y el respaldo para asegurar que los nuevos sistemas funcionan adecuadamente, tengan controles adecuados para la detección de problemas y estén debidamente documentados para que se tenga registros para su reconstrucción en caso de urgencia; y que el respaldo de soporte sea adecuado.

Discutirá las recomendaciones de auditoría con el personal del área que se esté auditando antes de preparar el informe.

Ayudará en la preparación de estudios de factibilidad y en investigaciones básicas realizadas con departamentos externos, para el desarrollo de nuevos sistemas de procesamiento de datos o la expansión de los actuales.

Evaluará y asistirá en el diseño de sistemas de PED para asegurar el uso más efectivo de las técnicas y equipos de control. Consultará con los supervisores y otros niveles de la gerencia sobre controles apropiados para los sistemas de procesamiento de datos.

Verificará el funcionamiento de los sistemas computarizados existentes mediante pruebas para determinar si los controles son adecuados y están operando correctamente.

Utilizará la computadora como una herramienta de auditoría para la selección y operación de técnicas de auditoría de la computadora y de los paquetes de software con el propósito de mejorar el alcance y la eficiencia de las auditorías.

Tiene la responsabilidad de ayudar al personal de auditoría de finanzas en aquellos aspectos de sus auditorías orientados hacia las operaciones de PED.

Preparará informes completos y detallados sobre las auditorías y recomendará los pasos requeridos para corregir variaciones, inconsistencias o métodos y procedimientos inexactos que estén en uso.

Revisará las operaciones de los departamentos para verificar la eficiencia de los controles internos sobre las funciones realizadas dentro de esa operación.

Experiencia Requerida

Conocimiento técnico cabal del análisis, diseño, revisión e implementación de las aplicaciones, para esto deberá tener :

- Familiarización general con los sistemas de cómputo, su análisis y diseño. Conocimiento de un lenguaje de programación.
- Comprensión básica de la lógica y conocimiento de los datos de la computadora, su seguridad y operaciones.

- **Comprensión general de los procedimientos, métodos y filosofías de la contabilidad y el control.**
- **Conocimiento práctico de los conceptos básicos de la auditoría y prácticas avanzadas.**
- **Capacidad de llevar al cabo las funciones de auditoría y de trabajar con la gerencia.**
- **Habilidad para dirigir, planificar, programar y supervisar funciones específicas.**
- **Habilidad para evaluar objetivamente.**
- **Aptitud para reconocer rápidamente problemas claves.**
- **Capacidad para comunicarse eficazmente.**
- **Una cantidad considerable de información debe obtenerse en un periodo de tiempo relativamente breve, de administradores, programadores y analistas. Asegurar y comprender esta información sin causar recelo exige fuertes habilidades interpersonales.**

Una función importante de la auditoría es la de identificar fuerzas mayores, problemas fundamentales y deficiencias claves.

1.1.5.OBJETIVOS DE LA AUDITORIA DE PED

El objetivo de una auditoría es predecir la confiabilidad y los riesgos relativos que debieran esperarse en el futuro en relación con el sistema que se encuentre operando. La imposición de los controles de operación diarios es una función propia de la gerencia en línea. El principal objetivo del auditor interno es evaluar los controles, verificar su implantación y proporcionar sus conclusiones a la gerencia.

El término "objetivos del control" tiene el mismo significado dentro de cualquier sistema de procesamiento de información, ya sea que se empleen o no computadoras; sin embargo, cuando se hace uso de la computadora se requiere hacer énfasis especial en cuanto a la naturaleza mecánica del procesamiento y la centralización de los archivos y operaciones.

Por lo anterior es importante mencionar que el CONTROL es todo aquello que tiende a causar la reducción de los riesgos. El control puede lograr esto reduciendo ya sea los efectos nocivos del riesgo o la frecuencia de su ocurrencia.

CAUSAS DE RIESGO

Los riesgos no surgen simplemente por falta de controles. Los riesgos son causados. Los controles actúan para reducir o eliminar estas causas; pero aún sin controles, necesariamente deben existir las causas antes de que se presenten los riesgos.

Una causa puede generar más de un tipo de riesgo. No existe una simple relación directa. Es más, los diversos riesgos que pueden derivarse de una causa en particular, normalmente no se presentarían con el mismo grado de probabilidad.

Existen tres tipos de controles

- 1) Preventivos
- 2) Detectivos
- 3) Correctivos

Preventivo

Los controles preventivos son aquellos que reducen la frecuencia con que ocurren las causas de riesgo. Un control preventivo actúa como una guía para ayudar a que las cosas sucedan como debe ser. Con frecuencia son pasivos y no implican ninguna actividad física directa. Este tipo de controles se encuentra a menudo tan sutilmente intercalados dentro de un proceso, que las personas involucradas en la operación pueden no estar siquiera conscientes de su existencia.

Detectivo

Un control detectivo no evita que una causa de riesgo ocurra, sino que dispara una alarma después de que ya ha ocurrido. El control detectivo puede poner fin al proceso posterior o simplemente registrar la ocurrencia. Esta función de vigilancia con frecuencia es bastante confiable; sin embargo, la detección de que una causa ha ocurrido es simplemente esa y nada más. Los controles detectivos alteran a las personas involucradas en el proceso, a fin de que estén conscientes de la existencia de un problema. Tal conocimiento es imprescindible si ha de seguirse la acción correspondiente para corregir los efectos de la causa detectada.

Correctivo

No es suficiente la simple detección de una causa de riesgo. Cuando se detectan tales situaciones, debe tomarse una decisión respecto a cuál es la acción correctiva apropiada, y posteriormente debe llevarse al cabo dicha acción. Este ayuda en la investigación y corrección de las causas de riesgo detectadas. La acción correctiva siempre es necesaria para remediar las causas de riesgo que se detectan. En ciertas ocasiones puede decirse que no vale la pena seguir una acción correctiva, pero tal decisión debe tomarse consciente y consistentemente.

En los sistemas de información, como en cualquier otra parte, cada control tiene un factor de costo. Ningún control debe costar más que los errores potenciales para cuya detección, prevención o corrección se establece.

Areas de Control

Las áreas de control dentro de un sistema computarizado incluyen :

Las aplicaciones incluyen todas las funciones de información del negocio, en cuyo procesamiento interviene una computadora. Los sistemas de aplicación abarcan uno o más departamentos de la organización, así como la operación de la computadora y el desarrollo de sistemas.

- Controles de aplicación, los cuales son peculiares a los sistemas de los usuarios individuales.

El desarrollo de sistemas cubre las actividades de los analistas de sistemas y programadores, quienes desarrollan y modifican archivos de las aplicaciones, los programas de computadora y otros procedimientos.

- Controles de desarrollo de sistemas, los cuales aseguran que la planeación y el desarrollo de sistemas se lleve al cabo en forma sistemática.

La instalación de procesamiento de información abarca todas las actividades relativas al equipo de cómputo y los archivos de información. Esto comprende la operación del computador, la biblioteca de los archivos, el equipo de captura de datos y la distribución de información.

- Controles de la instalación de procesamiento de información, los cuales se refieren al lugar físico en donde se lleva al cabo el procesamiento y cómo se procesan la mayor parte o todas las aplicaciones dentro de esa instalación.

- Controles en las redes de comunicaciones los cuales deben de asegurar la seguridad e integridad de la información.

1.1.6. PLANEACION DE AUDITORIA

Como en toda actividad, los mejores resultados los obtiene el que sabe que es lo que va a hacer y cómo ha de hacerlo, es decir, quien planea su trabajo.

La planeación tiene una importancia fundamental en auditoría, para poder planear una auditoría específica es necesario, aunque resulte obvio, fijar claramente dos situaciones: Que el servicio quede claramente contratado y que se tenga conciencia plena de que se esta en actitud de presentarse.

Planear el trabajo de auditoría, es conocer previamente cuáles son los procedimientos de auditoría que van a emplear, cuál es la extensión que va a darse a esas pruebas, en qué oportunidad se van a aplicar y cuáles son los papeles de trabajo en que se registrarán los resultados.

FASES DE LA PLANEACION DE AUDITORIA

- 1a. Investigación de aspectos generales y particulares de la empresa a examinar.

Comprende el estudio de todas aquellas cosas que hacen distintiva a la empresa que habremos de auditar, para poder decidir los aspectos específicos que deberá cubrir la planeación de dicha auditoría.

- 2a. Estudio y evaluación del control.

Desde el punto de vista técnico esta es la fase de planeación mas importante e implica el conocimiento formal de los métodos y rutinas que la empresa tiene establecidos para su operación y administración.

- 3a. Programación del trabajo de detalle específicamente aplicable.

Formulación del programa de trabajo que indique, punto por punto cada uno de los trabajos específicos a realizar para la obtención de evidencia suficiente y competente que apoye las conclusiones de la revisión, sobre las que se base la opinión final.

1.2. CONCEPTOS DE TELECOMUNICACIONES

Las Redes de Comunicaciones de datos son todos aquellos sistemas computacionales cuyos procesadores y terminales no coinciden geográficamente y la información o datos fluye entre ellos a través de algún sistema de telecomunicación.

En la actualidad las telecomunicaciones son un punto vital en los sistemas de procesamiento de datos, ya que el tener acceso a información de diferentes puntos es una realidad.

Por lo anterior, para la auditoría es de suma importancia tener conocimiento de algunos conceptos de telecomunicaciones. El objetivo de este subcapítulo es presentar en forma sencilla un conjunto de conceptos con la intención de que puedan servir de herramientas de análisis en la auditoría de sistemas de comunicación.

En primer lugar, diremos que Telecomunicación es la comunicación a distancia, por lo tanto, un sistema de telecomunicaciones es un conjunto de elementos relacionados entre sí para lograr la comunicación entre dos o más puntos distantes.

1.2.1. ANTECEDENTES HISTORICOS

El arte de la comunicación es tan antiguo como la humanidad. En la antigüedad se usaban tambores y humo para transmitir información entre localidades. A medida que pasó el tiempo se crearon nuevas técnicas y evolucionaron.

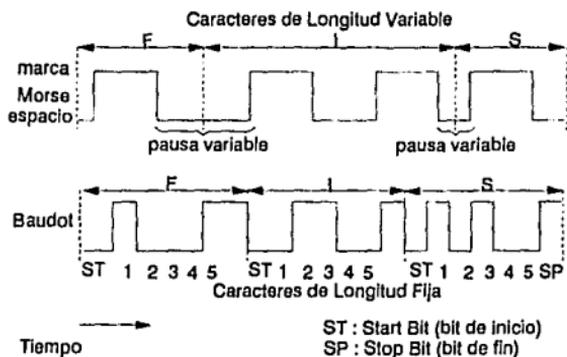
El Telégrafo.

La era de la comunicación electrónica se inició en 1834 con el invento del telégrafo, y su código asociado, que debemos a Samuel Morse. El código Morse utilizaba un número variable de elementos (puntos y rayas) con el objeto de definir cada carácter.

El invento del telégrafo adelantó la posibilidad de comunicación humana; sin embargo, tenía algunas limitaciones. Una de ellas fue no poder automatizar la transmisión. Debido a la incapacidad técnica de sincronizar unidades de envío y recepción automática. El uso de la telegrafía estuvo limitado a claves manuales hasta los primeros años del siglo XX.

Código Baudot

En el año de 1874, Emil Baudot en Francia ideó un código en el cual el número de elementos (bits) en una señal era el mismo para cada carácter y la duración (sincronización) de cada elemento era constante. Ese código fue llamado de longitud constante.



Comparación de los Códigos Morse y Baudot

En 1910, un americano llamado Howard Krum introdujo mejoras en el concepto de sincronización y lo aplicó al código de longitud constante de Baudot. Este desarrollo, llamado sincronización start/stop, condujo a la rápida difusión del uso de equipos automáticos de telegrafía.

En 1928, las teleimpresoras habían sido completamente mecanizadas, incorporaban un lector y un perforador de cinta de papel accionado por teclado; transmitían directamente por medio del teclado o a través de la cinta y el producto final era cinta perforada o bien, copia impresa.

Esta clase de equipo teleimpresor mecánico originalmente empleaba el código de 5 niveles de Baudot y operaba a velocidades de 45 a 75 bits por segundo. Más tarde se introdujeron versiones de código ASCII de 8 niveles que operaban a 110 bps. Pero, hasta 1970 se instalaron en todo el mundo mayor cantidad de dispositivos que empleaban el código de Baudot, de 100 años de antigüedad, que dispositivos que empleaban cualquier otro código.

Origen de los Protocolos

El primer equipo teleimpresor operaba sin ningún protocolo identificable, se alineaba el mensaje de cinta o se introducía el mensaje por medio del teclado (suponiendo que la máquina receptora en el otro extremo de la línea estuviera lista). Tan pronto como la máquina local comenzaba a transmitir, la máquina receptora copiaba la transmisión. (Tal sistema se llama "no controlado" o de "rueda libre"). A medida que las comunicaciones se volvieron más sofisticadas, al principio de los 50's se introdujeron dispositivos electromecánicos centrales para realizar tareas como invitación (notificando en secuencia a cada estación del mismo circuito para transmitir su tráfico) y selección (notificando a una determinada estación que debe recibir un mensaje). Para adaptarse al control adicional requerido para esta función, se equipó a las teleimpresoras con dispositivos que decodificaban secuencias de caracteres. Esto permitió a la teleimpresora enviar, recibir, reacondicionar o realizar alguna otra función básica. Dado que la mayoría de estas teleimpresoras operaban con el código Baudot, que no permite realizar funciones de control (excepto "alimentación de línea" y "retorno de carro"), se usaban series de caracteres alfabéticos diferentes llamadas "secuencias de control" para comandos de control específico.

El Teléfono

Paralelamente al desarrollo del telégrafo tuvo lugar el desarrollo del teléfono. El primer teléfono para uso comercial se instaló en 1877. Este sistema tenía un tablero manual. Permitía la comunicación por medio de la voz a través de la misma línea, valiéndose de comunicación alternada.

Alrededor de 1908, el sistema telefónico se había difundido por casi la totalidad de U.S.A. Así, alrededor de 1920, se habían establecido los principios básicos de telecomunicaciones, conmutación de mensajes y control de línea. Los sistemas se construyeron con base en comunicaciones a través de la voz y transmisión (ST/SP) de caracteres de datos. Luego de la Segunda Guerra Mundial comenzó el desarrollo comercial de la computadora. Como estas primeras máquinas eran orientadas a lotes, no existía la necesidad de interconectarse con el sistema de comunicación que abarcaba toda la nación; sin embargo, más adelante la industria tomó conciencia de la conveniencia de que máquinas y gente hablaran entre sí. Dado que el único sistema de comunicación disponible era el telefónico, naturalmente, las computadoras en evolución, habrían de desarrollarse siguiendo vías que les permitiera usar este servicio.

Comunicaciones y Computadoras

Entre tanto, el crecimiento del uso de la comunicación fue simultáneo al crecimiento de la tecnología de las computadoras y en parte, favorecido por él. Las redes de conmutación de mensajes, reservación y transacciones financieras de los años 50's y 60's usaban computadoras centralizadas comparativamente sofisticadas para controlar grandes poblaciones de dispositivos y terminales primitivas. A medida que esas redes crecían en lo que se refiere a volúmenes de tráfico y poblaciones de terminales, el aspecto "no controlado" de la operación de las terminales se volvió inaceptable. Luego de muchos estudios, los diseñadores del sistema finalmente determinaron que las terminales destinadas a la operación en redes basadas en computadoras debían permitir un grado de control más depurado que el alcanzado por los primeros métodos basados en la electromecánica.

En los años 60's las aplicaciones de comunicación de datos se expandieron más allá del intercambio rutinario de tráfico de mensajes. Los patrones de tráfico, la extensión de los mensajes, los requerimientos de tiempo de respuesta y los parámetros relacionados con estas nuevas aplicaciones, fueron significativamente diferentes de las primeras aplicaciones. Esto condujo a la necesidad de nuevas técnicas de transmisión. Con la tecnología disponible se lograron velocidades más altas, más terminales en un circuito dado, mejor control de errores y otras mejoras.

1.2.2. DEFINICIONES BASICAS

Tipos de Procesamiento

En la actualidad dos ambientes interrelacionados son dominantes :

- Definición global de los datos
(Bases de datos)
- Transporte global de los datos
(Redes)

Estos se han convertido en la parte principal de la concepción moderna de un sistema de procesamiento electrónico de datos.

Intimamente atados al transporte de los datos, están los conceptos de Telecomunicaciones y Teleprocesamiento. El primero, **telecomunicaciones**, hace referencia a la transmisión de datos a distancia usualmente por medios electrónicos. El **teleprocesamiento** en cambio, es una forma de intercambio de información en la cual un sistema de computación utiliza facilidades de comunicación, para obtener un resultado, según una secuencia de tareas predeterminadas (programas), a partir de una cierta cantidad de materia prima (datos).

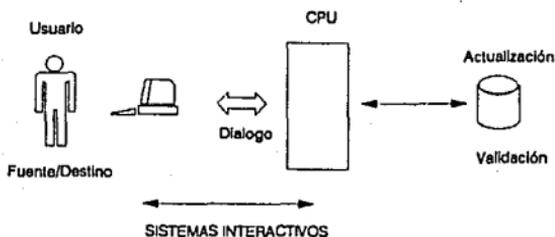
En el tema de las redes de procesamiento de datos, son muchos los conceptos que intuitivamente manejamos, algunos de los más importantes son los siguientes:

Un **Sistema en Línea** es aquél que recibe los datos directamente del punto de su generación y transmite la salida directamente al usuario final. A su vez, un sistema en tiempo real recibe el ingreso desde el ambiente (o evento), procesa con demora mínima (incluyendo la actualización de archivos) y transmite la respuesta (salida) a tiempo, para afectar el ambiente o controlar el evento en curso.

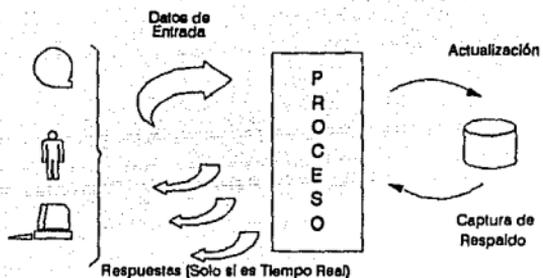
Un sistema interactivo ha sido mencionado como una aplicación comercial de los principios de tiempo real.

Es claro que un sistema interactivo recibe la entrada directamente desde el punto de la generación de los datos. También, en general, se procesa la entrada a nivel de "campo". Otra característica es que los errores son detectados y corregidos por cada dato que entra, en el mismo momento de su ingreso y con notificación al usuario final. Los sistemas operativos que soportan esta filosofía proveen instrucciones operativas incluidas en los procedimientos conversacionales típicos en estos casos.

La modalidad de trabajo conocida como consulta, permite el acceso directo del usuario final a los archivos del sistema, mediante una interacción familiar al usuario.

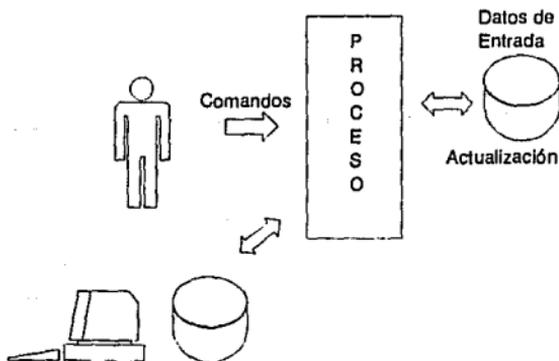


Una forma de trabajar en la actualidad es el **procesamiento transaccional**. Este está muy vinculado al objeto de este trabajo, ya que muchas redes operan con esta filosofía. El procesamiento transaccional permite que la unidad de comunicaciones y procesamiento sea reducida del nivel lote al nivel transacción. Generalmente, se parte de una secuencia corta de datos de entrada, que supuestamente contiene toda la información necesaria para el proceso. Los errores del ingreso son detectados y corregidos en la fuente, antes de que el archivo sea afectado. Puede, o no, ser tiempo real. Una vez realizado el procesamiento de los datos de entrada (incluyendo cálculos y actualización), se retornan uno o varios mensajes hacia el punto de origen de los datos (en el caso de tiempo real) y normalmente se lleva una bitácora en la que se registran cronológicamente todas las transacciones.



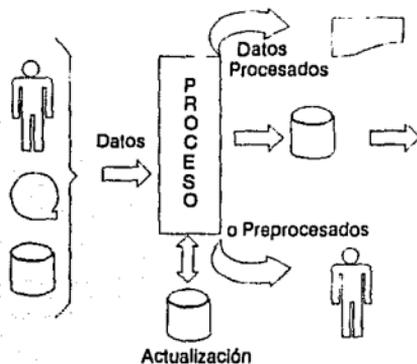
PROCESAMIENTO TRANSACCIONAL

Es muy común en comunicaciones de datos, mencionar la **entrada remota de trabajos**. Esta forma de procesamiento permite la presentación remota de comandos para ejecución de tareas o procesos específicos a realizarse en un sistema central. Puede o no, involucrar la entrada/salida remota de datos.



ENTRADA REMOTA DE TRABAJOS

No se debe confundir lo anterior con la **entrada remota de lotes**. Esta modalidad permite la presentación remota de lotes de datos para procesamiento y actualización de archivos en un sistema central. Se pueden usar técnicas para transmisión de datos preprocesados desde central a lugares remotos mediante el uso de dispositivos periféricos adecuados.

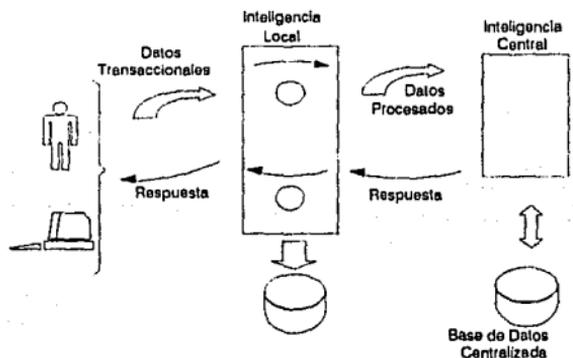


ENTRADA REMOTA DE LOTES

Pero en la actualidad uno de los conceptos más importantes, es el **procesamiento distribuido**. Este implica la disponibilidad de facilidades de procesamiento en estaciones "exteriores". La distribución de la inteligencia se puede realizar sobre una base geográfica y organizacional. Estas facilidades reubicadas remotamente pueden operar en cualquiera de muchos niveles, por ejemplo:

- Almacenamiento intermedio y validación de la entrada
- Control de la red
- Procesamiento de archivos locales
- Respaldo total o parcial de las facilidades centrales

El surgimiento de una gran miniaturización, la disminución de los costos y la "moda" de la computación a todos los niveles, ha llevado el Procesamiento Distribuido de Datos (PDD) desde el estrato teórico a una realidad total; sin embargo, si lo enfocamos desde el punto de vista comercial o industrial, todavía debemos hacer algunos comentarios adicionales. En muchas aplicaciones comerciales actuales, la distribución del procesamiento no implica la distribución de la base de datos, es decir, se dispone de inteligencia local, pero se sigue dependiendo de una base central para poder satisfacer un requerimiento.



PROCESAMIENTO DE TRANSACCIONES CON INTELIGENCIA LOCAL Y REMOTA

Otra modalidad que va tomando más fuerza, aunque lentamente por factores de confiabilidad en las comunicaciones, es el procesamiento distribuido de datos distribuidos (PDDD).

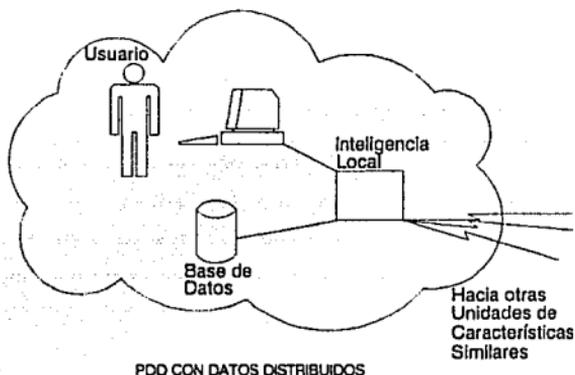
En este caso :

Datos Locales (Distribuidos)	+	Red Comunicaciones	=	Base de Datos Lógicamente Centralizada
------------------------------------	---	-----------------------	---	--

Los datos se ubican físicamente en los puntos (remotos) en donde éstos se originan y porcentualmente se usan más.

Mediante adecuadas facilidades de comunicación (que deben incluir no sólo los medios físicos, sino un rico conjunto de funciones y servicios al usuario remoto, además de las indispensables garantías), se logra la unión de los datos distribuidos en una única base de datos centralizada lógicamente.

En estos casos debe buscarse un mínimo en el número de "operaciones cruzadas" entre dependencias remotas.



Otra forma de trabajo actual en redes de comunicaciones de datos, se llama **conmutación de mensajes (Message Switching)**. Este término, usualmente se explica en oposición a la conmutación de circuitos, vieja técnica telefónica.

La conmutación de mensajes está relacionada con una técnica de procesamiento en nodos de la red, conocido como "almacena y prosiga" (store & forward). La entrada, como se recibió en el nodo para la transmisión, es almacenada un cierto tiempo, el cual depende de la disponibilidad de las propias líneas de salida. No se dispone de una conexión física preestablecida entre la fuente original y el destino final, sino que esta asignación de ruta física es una función dinámica.

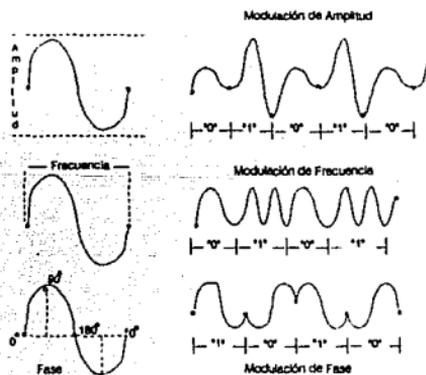
Asociado a este concepto, existe otro llamado **conmutación de paquetes**. Es un desarrollo de la conmutación de mensajes, en donde éstos se dividen en paquetes (segmentos), separados, que son ruteados independientemente a su destino. Esto mejora los niveles de carga y el balanceo de los dispositivos terminales (DTE: Data Terminal Equipment), con grandes ganancias extras en el rendimiento de la red y su transparencia.

Tipos de Modulación de Señal

Las señales de banda base producidas por diferentes fuentes de información no son adecuadas para la transmisión directa a través de un canal asignado. Estas señales son en ocasiones fuertemente modificadas para facilitar su transmisión. Este proceso de conversión se conoce como modulación. En esta técnica, se utiliza la señal de banda base para modificar algún parámetro de una señal portadora de alta frecuencia.

Una portadora es una senoide de alta frecuencia, y uno de sus parámetros tal como la amplitud, la frecuencia o la fase se varía en proporción a la señal de banda base. De acuerdo con esto, se obtiene Modulación en Amplitud (AM), la Modulación en Frecuencia (FM) o la Modulación en Fase (MP):

Las siguientes gráficas muestran las diferencias en la forma de modular una señal a efectos de que transporte información de naturaleza binaria.



Baudío (Baud)

El baudío es una unidad de velocidad de señalización igual a 1 dividido por el tiempo de duración del pulso o unidad más corta existente en cualquier carácter :

$$1 \text{ baudío} = 1 / t_p$$

Velocidad en Baudios (Baud Rate)

Es el número de elementos de señalización por segundo.

$$1 \text{ baudío} = 1 \text{ bit por segundo (bps), si cada elemento de señal transporta 1 bit.}$$

Si hay 4 elementos de señalización diferentes, cada elemento puede transportar 2 bits y 1 bps = 2 baudios.

Si hay 8 elementos, 1 bps = 3 baudios

Si hay 16 elementos, 1 bps = 4 baudios

En general, si hay m elementos, 1 bps = $(\log_2 m)$ baudios.

Capacidad de un Canal de Comunicaciones

Es el número de bits/seg, que un canal puede transportar.

Shannon, demostró que existe una velocidad máxima de transmisión de dígitos binarios por un canal de banda limitada a BW hertz, con una potencia promedio de ruido N y una potencia de señal S . Esta velocidad de transmisión, o capacidad C , es máxima en el sentido de que si se trata de transmitir información a una velocidad superior, el número de errores que se presentan al decodificar las señales en el receptor comienza a aumentar rápidamente.

La capacidad máxima de un canal según la Ley de Shannon es:

$$\text{Capacidad} = BW \cdot \log_2 (1 + S/N)$$

Donde :

BW = Band Width (ancho de banda)

S/N = Signal/Noise (relación señal/ruido)

Aumentado el ancho de banda, mejora la capacidad.

Clasificación de Circuitos

En U.S.A. se aplica la siguiente clasificación de los circuitos en servicios de transmisión públicos :

- Banda angosta, con velocidades hasta 150 bps, disponible para operaciones de teletipo a baja velocidad.
- Grado de voz, con velocidades hasta 9600 bps. Altamente usado para comunicaciones de datos. Permite punto a punto o multipunto a menor velocidad. Pueden obtenerse 19.2 kbps usando bplexores, que combinan dos líneas de 9.6 kbps.
- Canales de banda ancha, derivados de la combinación de grupos de banda de voz. Admiten velocidades de 19.2 kbps, 40.8 kbps, 50 kbps y 230.4 kbps (alto costo).
- Servicios digitales (DDS : Dataphone Digital Services). Fueron introducidos por Bell en 1974 y están disponibles en muchas ciudades. Tienen una baja tasa de error garantizada y permiten :

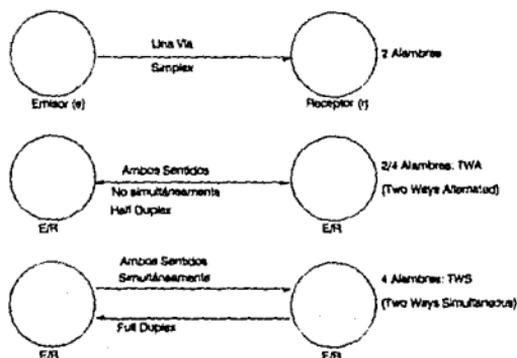
2.4 kbps
4.8 kbps
9.6 kbps
56 kbps

Por tratarse de transmisiones digitales no se requieren modems. Se usa una Unidad de Servicio de Datos (DSU Data Service Unit) para efectos de la conexión.

Circuitos y Modos de Operación

En el pasado, los términos "Half Duplex" (HDX) y "Full Duplex" (FDX) se relacionaban básicamente con la cantidad de alambres (HDX: 2; FDX: 4) y el tipo de interacción de los mensajes u operación, donde HDX se refería a dos vías alternadas (TWA : Two Ways Alternated) y FDX a dos vías simultáneas (TWS : Two Ways Simultaneous). Los términos TWA y TWS han sido adoptados para describir la Operación de las líneas.

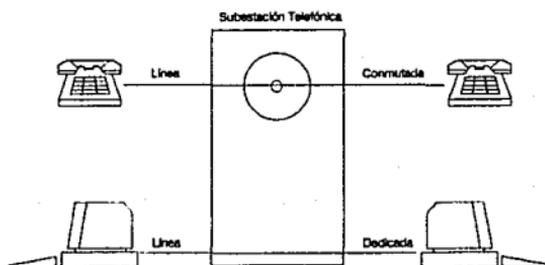
- Líneas HDX/Operación TWA. La transmisión tiene lugar en ambos sentidos pero no simultáneamente. Esta forma tiene el inconveniente de una gran demora por inversión de línea (Turn-Around) que puede llegar a 150 ms o más, y por consiguiente no siempre es aplicable a sistemas en línea en tiempo real.
- Líneas HDX/Operación TWS. La transmisión se realiza en ambos sentidos simultáneamente, sobre dos alambres, a través de una división del ancho de banda en canales de distinta frecuencia. Esto implica un equipo de conexión más costoso; sin embargo, por las ventajas que tiene, su uso va en aumento.
- Líneas FDX/Operación TWA. Cada par de alambres se destina a la transmisión en un sentido. Por lo tanto, se permiten ambos pero no simultáneamente. De esta forma se reduce casi a cero el tiempo de inversión de línea. Este sistema por ser relativamente barato debido a su simplicidad y bastante eficiencia, es muy usado.
- Líneas FDX/Operación TWS. Esta es la forma más eficiente de utilización de las líneas. La Operación simultánea en ambos sentidos lo hace muy adecuado en aplicaciones interactivas.



REPRESENTACION ESQUEMATICA DE LOS CONCEPTOS HDX, FDX, SPX, TWA y TWS

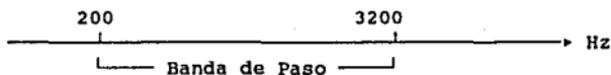
Líneas Privadas (Dedicadas) y Conmutadas

Una subestación de teléfonos puede proveer líneas dedicadas (privadas) y líneas conmutadas (públicas o discadas). La siguiente figura ilustra los tipos de conexiones físicas.



Banda de Paso

Representado por dos números que indican la frecuencia máxima y mínima a las que responde el circuito.

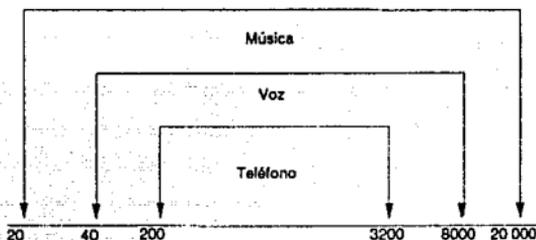


Ancho de Banda

Es un número que representa el rango de frecuencia en consideración, sin especificar cuáles son sus límites inferior y superior. Se obtiene como diferencia entre los valores (máximo y mínimo) de la banda de paso.

$$3200 - 200 \text{ Hz} = 3000 \text{ Hz} = 3 \text{ KHz}$$

podría ser : $14 \text{ KHz} - 11 \text{ KHz} = 3 \text{ KHz}$



BANDA DE PASO CORRESPONDIENTE AL TELEFONO, VOZ Y MUSICA

Sondeo(Polling)

Imaginemos una situación en la cual dos personas se encuentran intercambiando opiniones. Es lógico suponer que en este intercambio o diálogo, cada vez que uno de los participantes comienza a hablar, el otro se detiene y escucha o atiende lo que le dicen.

De una forma similar, se procede en un enlace punto a punto entre una computadora y una terminal operada por un usuario. Cuando la terminal elemento de menor jerarquía potencial quiere transmitir datos, lo hace interrumpiendo al procesador central. La operación inversa también se cumple. Internamente en el procesador, existe una lógica implementada en el software central, que interactuando con el adaptador de comunicaciones y otros elementos físicos de arbitraje, permiten que estas interrupciones se realicen bajo control de los mismos.

Esta forma conversacional no es aplicable en un grupo grande de terminales, ni tampoco de personas. En una asamblea, el procedimiento más común consiste en "pedir la palabra" al secretario de la mesa coordinadora y esperar su turno en una lista. En un enlace de comunicaciones de datos, el procedimiento es similar, pero se diferencia en que las terminales (personas) no piden la palabra sino que esperan a ser invitadas a transmitir (intervenir). El procedimiento se llama "sondeo" y podríamos esquematizarlo como sigue :

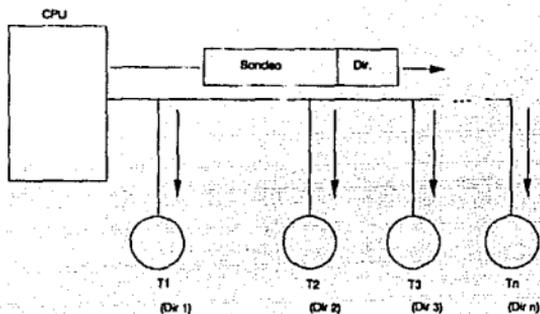
1. Se definió una tabla(I) con las direcciones de las terminales que van a intervenir.
2. Se define el orden de intervención de las mismas, estableciéndose prioridades si así se desea (tabla II).
3. Se definen los elementos de control y almacenamiento que se usarán (buffers, reintentos, mensajes, etc.) para manejar el tráfico.
4. El elemento de control Sistema Central invita, una a la vez, a las terminales a transmitir, según el orden de la tabla II, direccionando según la tabla I.
5. Estas responden negativamente a la invitación, o hacen uso de ella enviando los datos.
6. Se reitera el procedimiento mientras existan entradas en la tabla II.

Existen Dos tipos Básico de Sondeo :

- Sondeo por llamado a lista (Roll Call Polling)
- Sondeo en secuencia (Hub Polling)

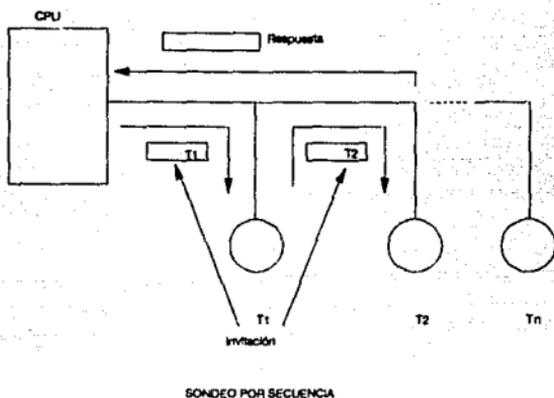
En el primer caso, el elemento central envía un mensaje de invitación a la primera estación del enlace (1^o posición de la tabla II). Este mensaje lleva los caracteres de invitación (EOT, ENQ en ISO asincrono) más la dirección de la terminal encuestada. Si la terminal no tiene datos para enviar, retorna un mensaje explicatorio (EOT).

Ante la negativa, el elemento central envía un mensaje de sondeo a la 2^o terminal y así sucesivamente. En este caso, el adaptador de la terminal encuestada no necesita tener demasiada inteligencia residente, lo cual reduce el costo.



SONDEO POR LLAMADO A LISTA

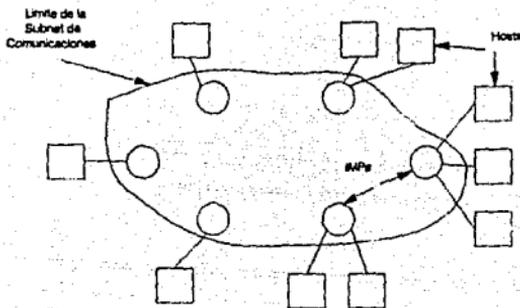
En el (sondeo por secuencia), por el contrario, del sistema central parte un mensaje de sondeo destinado a la primera estación del enlace y ésta, luego de reconocerlo, si no tiene datos para transmitir, le cambiará la dirección de destino y lo enviará a la segunda terminal. La secuencia se repite hasta agotar las terminales en la lista o hasta que una conteste. De esta forma se evita la intervención del CPU en las invitaciones infructuosas (que generalmente son las más comunes). Se obtiene un mejor rendimiento del sistema central, pero se necesita más inteligencia en la interconexión de cada terminal, lo que aumenta los costos.



1.2.3. ESTRUCTURAS DE LAS REDES

En todas las redes existen máquinas donde los usuarios corren sus aplicaciones, siguiendo la terminología de una de las más grandes redes, ARPANET, estas máquinas son llamadas Host. Los Host se conectan a la subnet de comunicación. El trabajo de la subnet es transportar mensajes de un host a otro, del mismo modo que el sistema telefónico acarrea palabras de un lado a otro. Si separamos el aspecto de comunicaciones (Subnet) del aspecto de aplicaciones (Host), el diseño de la red se simplifica.

La subnet consiste principalmente de 2 elementos: elementos de conmutación y líneas de transmisión, los elementos de conmutación son generalmente computadoras especializadas. En ARPANET son llamados IMPs (Interface Message Processors), pero también se conocen como computadoras de comunicación, paquetes de switcheo o nodos. Las líneas de transmisión son llamadas circuitos o canales.



RELACION ENTRE LOS HOSTS Y LA SUBNET

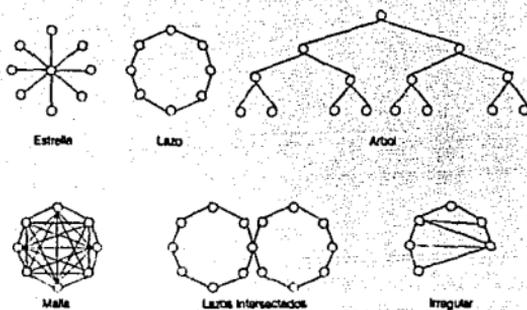
Un host es conectado a un IMP(a veces varios). Toda la comunicación de el host es vía IMP.

Existen en general dos tipos de diseños para la subnet de comunicaciones:

1. Canales punto a punto.
2. Radicación de canales.

En el primero, la red tiene muchos cables o canales de líneas telefónicas, cada línea conecta un par de IMPs. Si dos IMPs no tienen un cable que los una, la comunicación se hace vía otro IMP. Cuando un mensaje es enviado desde un IMP a otro vía uno o varios IMPs intermedios, cargan el mensaje mientras la línea de salida se libera y entonces lo envía. La subnet que usa este principio es llamada punto a punto o carga-y-envía.

Cuando se usa una subnet punto a punto un importante dilema es que topología de conexión de IMPs queremos tener, la siguiente figura nos muestra las diferentes posibilidades.

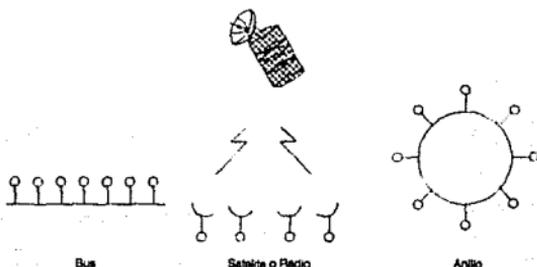


POSIBLES TOPOLOGIAS PARA SUBNETS PUNTO A PUNTO

Las redes locales son diseñadas con una topología simétrica. En contraste, con las topologías irregulares que usualmente son el resultado de conectar computadoras vía red telefónica.

El segundo tipo de arquitectura de comunicaciones es la radiación o difusión. En este diseño se usa un canal de comunicaciones compartido por todos los IMPs. Un mensaje es enviado por un IMP y el mensaje es recibido en todos los IMPs. El mensaje lleva la especificación de para quién es el mensaje y los demás IMPs lo ignoran.

La siguiente figura muestra las posibles conexiones para este diseño.



SUBNETS DE COMUNICACIONES RADIADAS

En la red con Bus o cable, en un instante una máquina es la maestra del bus y puede transmitir, todas las otras máquinas deben abstenerse de mandar mensajes. Un bus debe tener un mecanismo para resolver conflictos cuando dos o más IMPs quieren transmitir simultáneamente.

Una segunda posibilidad es un satélite o un sistema de radio terrestre, en los cuales cada IMP tiene una antena con la cual envía y recibe mensajes, todos los IMPs pueden oír la salida del satélite.

El tercer sistema de radiación es el de anillo, en éste, todos los bits se propagan alrededor del anillo, no esperan el resto del mensaje para salir todos juntos, en contraste con un lazo, el mensaje no es retransmitido por el siguiente IMP.

La subnet de radiación se puede dividir también en estática o dinámica, la primera divide pequeños intervalos de tiempo y hace un "round robin", es decir, cada IMP puede enviar cuando es su turno, esto desperdicia el canal de transmisión cuando algunos IMPs no tienen que transmitir. El método dinámico es centralizado o descentralizado. Un canal centralizado es un simple mecanismo, por ejemplo una unidad aleatoria, la cual determina cuál es el siguiente, esta unidad puede recibir peticiones y tomar decisiones con base en un algoritmo. En el canal descentralizado cada IMP puede decidir cuando transmitir o no.

1.3. ANTECEDENTES DE LA BANCA

Dado que el objeto de estudio es auditar a la Red de Telecomunicaciones de una Sociedad Nacional de Crédito, es importante conocer los siguientes aspectos básicos de estas sociedades.

1.3.1 ANTECEDENTES HISTORICOS DE LA BANCA

En un principio hubo dos tipos de banca : la comercial y la de inversión que poco tiempo después se unieron para formar la multibanca.

Banca Comercial

Era la institución (Sociedad Anónima), a la cual el gobierno federal por conducto de la Secretaria de Hacienda y Crédito Público le había otorgado la concesión, para celebrar operaciones de depósito, ahorro y fiduciario referentes al comercio en general.

Banca de Inversión

Eran las sociedades financieras e hipotecarias constituidas con la finalidad principal de efectuar operaciones de financiamiento e inversiones.

Multibanca

Era la unión de la banca comercial y la banca de inversión en una sola localidad pero controlando por separado sus operaciones por cada tipo de actividad (Depósito, ahorro, financiero, hipotecario y fiduciario).

Aspectos Importantes del Sistema Financiero Mexicano

- 1864 - Primeros bancos enfocados al comercio y no a la producción.
- 1925 - Se crea el Banco de México.
- 1926 - Nacimiento de la Banca Nacional.
- 1932 - Ley General de Instituciones de Crédito y Organizaciones Auxiliares.
- 1940 - Ley Orgánica de Nacional Financiera.

- 1941 - Reforma de la Ley Bancaria.
- 1946 - Creación de la Comisión Nacional de Valores.
- 1953 - Ley de la Comisión Nacional de Valores.
- 1954 - Ley de las Sociedades de Inversión.
- 1975 - Ley del Mercado de Valores.
- 1977 - Primera emisión de Petrobonos.
- 1978 - Creación del Indeval.
- 1980 - Aceptaciones Bancarias.
- 1981 - Papel Comercial.
- 1982 - Expropiación Bancaria.
- 1985 - Aparecen las sociedades de Inversión de Renta Fija.
- 1986 - Sociedades de Inversión de Formación de Capitales
- 1989 - Bondes, Tesobonos, Liberación de tasas y Coeficientes de Liquidez, Bondis, (NAFINSA). Sociedades de Inversión, Personas morales, Ajustabono.
- 1990 - Iniciativa de Reprivatización de la Banca.

1.3.2. ESTRUCTURA BANCARIA NACIONAL ACTUAL

Con base en la cancelación de concesiones por el gobierno federal, el 1o. de septiembre de 1982, fueron nacionalizados 60 bancos privados, mismos que siguieron operando bajo su razón social, pero con directores nombrados por el ejecutivo federal.

Una vez nacionalizados se expidieron decretos a través de los cuales quedarón 29 instituciones a partir del 29 de agosto de 1983.

Decretos de transformación de bancos múltiples sociedades anónimas en bancos múltiples sociedades nacionales de crédito (17 bancos).

Decretos de transformación y fusión de bancos múltiples especializados y mixtos sociedades anónimas en sociedades nacionales de crédito (12 bancos).

Reordenación del Sistema Bancario

Posteriormente la Secretaría de Hacienda y Crédito Público, dentro del proceso de reordenación y racionalización del sistema bancario nacional, el 1o. de marzo de 1985, reduce de 29 a 20 las sociedades nacionales de crédito, quedando:

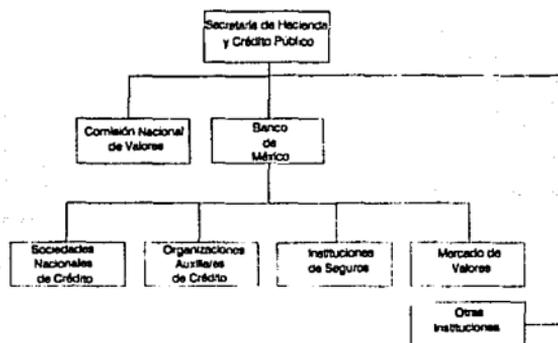
Seis sociedades nacionales de crédito con cobertura nacional.

Ocho sociedades de crédito con cobertura multiregional.

Seis sociedades nacionales de crédito con cobertura regional.

1.3.3. EL SISTEMA FINANCIERO MEXICANO

El sistema financiero mexicano comprende todas las instituciones financieras de México; éstas se dividen de acuerdo a sus operaciones especializadas de la siguiente forma :



SISTEMA FINANCIERO MEXICANO

Secretaría de Hacienda y Crédito Público

Es el organismo que determina las medidas relativas a la creación y funcionamiento de las Sociedades Nacionales de Crédito y las Organizaciones Auxiliares de Crédito.

Comisión Nacional Bancaria y de Seguros

Se encarga de la inspección y vigilancia de las instituciones de Crédito y Organizaciones Auxiliares, a través de la documentación que recibe de las mismas y de un cuerpo especializado de inspectores que efectúan visitas al domicilio de las mencionadas instituciones.

Banco de México

Actúa como regulador del crédito y del dinero. Tiene el control de la emisión de billetes, la regulación de la acuñación de la moneda y de la reserva metálica; asimismo, se encarga de administrar el encaje legal(*) y funge como cámara de compensación entre las instituciones.

Sociedades Nacionales de Crédito

La banca es una institución de Crédito que sirve de intermediaria entre las personas que en forma permanente u ocasional tienen capitales ociosos y aquéllas que lo solicitan para canalizarlo hacia fines productivos.

Es una institución de crédito que requiere de una "concesión" del gobierno federal, para poder realizar las operaciones que la ley cataloga como actividades de banca y crédito.

En una forma más general puede decirse que un banco es un punto de contacto entre personas que le confían su dinero y personas que lo solicitan a base de crédito. Se trata de entidades constituidas por la ley, como sociedades nacionales de crédito, que ejercen el crédito en forma masiva y profesional, de ahí que también se les conozca como instituciones de crédito.

La característica básica de toda institución de crédito es el papel de intermediación que desempeñan; captan por una parte recursos del público y los ponen a disposición de otras personas que lo requieran para beneficio de sus actividades productivas, de distribución o consumo.

Organizaciones Auxiliares de Crédito

Existen organizaciones auxiliares de crédito tanto públicas como privadas, siendo estas los almacenes de depósito, las uniones de crédito, las instituciones de fianzas y las arrendadoras.

(*) El encaje legal es el depósito (respaldo económico que garantiza las operaciones que efectúan los cuenta habientes) que dejan las instituciones de crédito en el Banco de México.

Las sociedades nacionales de crédito basan sus funciones en cuatro operaciones :

Activas
Pasivas
Contingentes
Servicio

Activo

El activo representa todos los bienes y derechos que son propiedad del banco.

Por operación activa se entiende aquella que efectúa el banco al invertir el dinero que recibió de terceras personas, poniéndole en condiciones de producir y por lo cual se constituye en acreedor de las personas a quienes se les proporciona.

En un sentido mas general pueden definirse como aquellas operaciones que realiza el banco al invertir, tanto los recursos propios, como los ajenos que maneja.

Pasivo

El pasivo representa todas las deudas y obligaciones del banco contraídas por terceras personas.

Por operación pasiva se entiende aquella que realiza un banco para captar dinero, esencialmente del público en general, por lo que se convierte en deudor de las personas que se lo facilitan. Desde el punto de vista contable y en un aspecto más general las operaciones pasivas podrían conceptuarse como aquellas que el banco registra en su pasivo.

Contingentes

Son aquellas que pueden traducirse para el banco en una obligación directa, al no cumplir una tercera persona la parte que le corresponde por dicha obligación.

Servicio

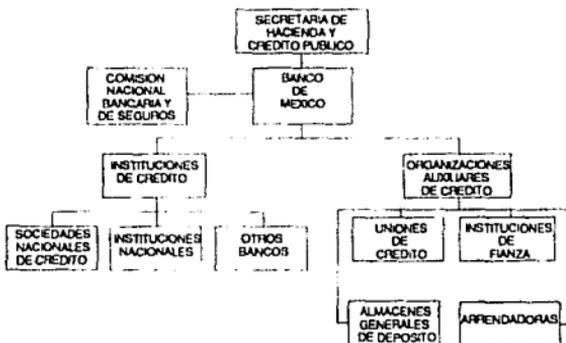
Existen otras operaciones que vienen a completar las operaciones básicas y de carácter contingente que realiza la banca y que tiene el propósito de ofrecer otros servicios a la clientela en general.

Instituciones de Seguros

La función específica de estas instituciones es proteger los bienes muebles e inmuebles, tanto de personas físicas y morales, asegurando el bienestar económico de los beneficiarios mediante la emisión del contrato de seguro respectivo. Existen instituciones de seguros nacionales e instituciones privadas.

Mercado de Valores

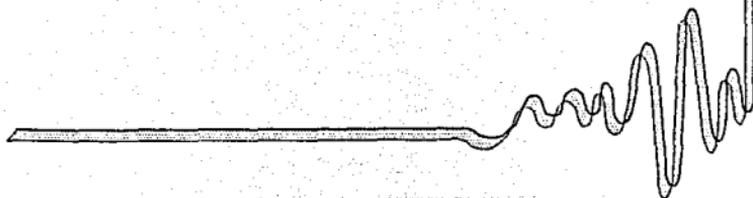
Con este nombre se conoce el ámbito de actividad de las llamadas instituciones bursátiles. La función principal de estas instituciones es regular la oferta pública de valores y las actividades intermediarias de compra y venta de los valores en el mercado.



SISTEMA BANCARIO MEXICANO

CAPITULO II

APLICACIONES Y COMPONENTES PRINCIPALES DE LA RED DE TELECOMUNICACIONES



CAPITULO II

APLICACIONES Y COMPONENTES PRINCIPALES DE LA RED DE TELECOMUNICACIONES

En el capítulo anterior se hizo una breve descripción de los conocimientos básicos de auditoría, telecomunicaciones y banca, en este mencionaremos el alcance de la auditoría y describiremos la metodología utilizada para cubrir el objetivo de conocer las aplicaciones y componentes principales de la red auditada.

2.1. ALCANCE DE LA AUDITORIA

La metodología presentada estará enfocada a los siguientes aspectos :

Seguridad de la Red
Eficiencia y Desempeño de la Red
Administración de la Red

La metodología presentada está compuesta de seis pasos en los cuales se cubre el alcance presentado, además, en esta forma se cuenta con un orden para poder analizar la información y poder dar una opinión de un aspecto específico de la auditoría. Los pasos son los siguientes :

PASO No. 1 Definir base instalada.

Determinar las aplicaciones y componentes principales de la red.

PASO No. 2 Evaluar la seguridad de la red.

Determinar la seguridad de la red en los diferentes niveles de la organización (Hardware, Software, Transmisión, Administrativa y Física). Además de revisar los planes de contingencia con que se cuenta.

PASO No. 3 Evaluar la eficiencia y desempeño de la red.

Para el desempeño determinar la disponibilidad, capacidad de transmisión, tiempo de respuesta, confiabilidad de la red, y para la eficiencia el costo promedio por transacción y por terminal conectada en la red.

PASO No. 4 Evaluar la administración de la red.

Definir los sistemas de administración y control de la red que se encuentran implantados.

Se cubrirá la administración de fallas, desempeño, configuración (hardware, software), servicios y la organización del área de comunicaciones.

PASO No. 5 Identificar los requerimientos futuros de telecomunicaciones.

PASO No. 6 Dictámen de la auditoría.

Análisis de la información obtenida, realización del documento final, discusión con los interesados y recomendaciones.

2.2. DEFINIR BASE INSTALADA

El primer paso de la auditoría definir la base instalada, tiene como finalidad determinar los componentes físicos, lógicos y las aplicaciones principales de la red.

Nuestro primer objetivo es conocer las aplicaciones bancarias que hacen uso de la red de telecomunicaciones y los porcentajes en que la utilizan cada una de ellas.

Para lo cual es necesario que el auditor tenga la siguiente información :

- ¿ Cuáles son las aplicaciones que utilizan la red ?
- ¿ Con qué frecuencia la utilizan ?
- ¿ Cuáles son los niveles de tráfico en cada aplicación ?
- Definir los servicios que ofrece la red.
- ¿ Cuáles de estos servicios se utilizan ?
- ¿ Cuál es el crecimiento estimado de tráfico por cada una de las aplicaciones en corto plazo ?
- ¿ Cuál es la razón por la que no se utilizan algunos servicios ?

En esta parte tenemos como objetivo recolectar la información necesaria para realizar el estudio de la red de telecomunicaciones a auditar :

En esta parte tenemos como objetivo recolectar la información necesaria para realizar el estudio de la red de telecomunicaciones a auditar :

- ¿ Se cuenta con un inventario de la red ?
- ¿ Quién lleva el inventario ?
- ¿ Cómo lo administra ?
- ¿ Qué información tiene ?
- ¿ Con qué frecuencia se actualiza el inventario ?
- Solicitar una copia del inventario de equipo.
- Solicitar copia de enlaces de la red.
- Solicitar diagrama de la red a auditar.

Para recolectar la información antes mencionada el auditor utilizará las técnicas de auditoría. A continuación se encuentra su descripción :

2.3. TECNICAS DE AUDITORIA

Estudio General.- Apreciación sobre las características generales de una organización, este estudio deberá aplicarse con mucho cuidado por lo que es recomendable que su aplicación la lleve al cabo un auditor con preparación, experiencia y madurez, para asegurar un juicio profesional sólido y amplio.

Análisis.- Clasificación y agrupación de los distintos elementos individuales que forman un evento, de tal manera que los grupos constituyan unidades homogéneas y significativas.

Inspección.- Examen físico de bienes materiales o documentaciones con objeto de cerciorarse de su autenticidad.

Confirmación.- Obtención de una comunicación escrita de una persona de la empresa o ajena a ella, pero que conozca la naturaleza y condiciones de la operación, para poder considerar la información presentada como válida.

Investigación.- Obtención de información, datos y comentarios de funcionarios, y empleados de la empresa.

Certificación.- Obtención de un documento con el que se asegure la verdad de un hecho, legalizado por lo general, con la firma de una autoridad.

Observación.- Presencia física de como se realizan ciertas operaciones o hechos.

Cálculo.- Verificación matemática de procedimientos.

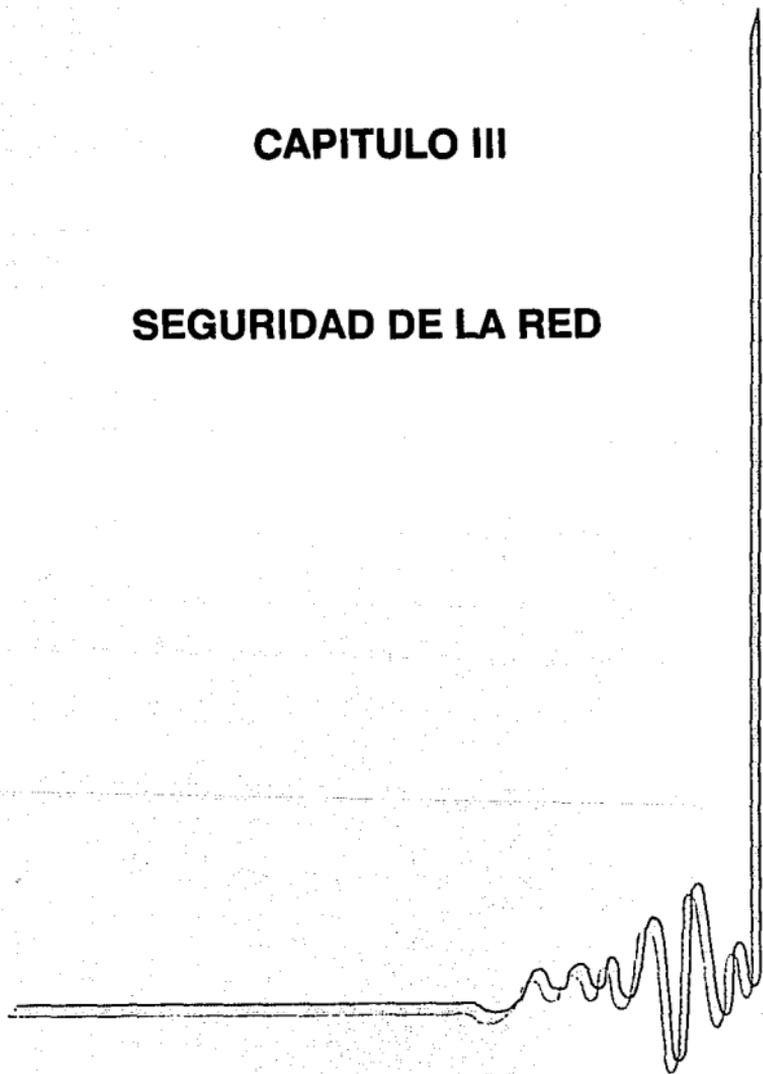
Para aplicar las técnicas antes mencionadas encontramos la utilización de :

- Cuestionarios y Encuestas.
- Entrevistas
- Revisión de documentación
- Manuales técnicos.

Las técnicas mencionadas serán la herramienta principal para la recolección de información, durante los cinco primeros pasos de la metodología.

CAPITULO III

SEGURIDAD DE LA RED



CAPITULO III

SEGURIDAD DE LA RED

En este capítulo se evaluará la seguridad de la red de telecomunicaciones. Los tópicos que se incluyen son la seguridad del hardware, software, transmisión y física (medio ambiente). Además, se revisará la administración de la red y en qué porcentaje se cubren los planes de contingencia.

La seguridad y la confiabilidad son las consideraciones primordiales al hacer la auditoría de cualquier sistema, cabe aclarar que su importancia es proporcional al valor y al volumen de tráfico de la red.

Por la importancia que han adquirido los sistemas de comunicaciones, hoy en día es tan necesario una auditoría en comunicaciones como en procesamiento electrónico de datos.

3.1. DEFINICION DE SISTEMA SEGURO

Un sistema de comunicaciones seguro, se define como un sistema automatizado en que una transacción (mensaje) :

- 1) Siempre se entrega a la estación de salida correcta.
- 2) Es recibida con el mismo contenido que se envió.
- 3) No puede ser conocida o retardada por ninguna persona sin autorización durante su transmisión.

En realidad, un sistema totalmente "Seguro" es inalcanzable. Es posible proporcionar niveles adecuados de seguridad, de acuerdo con los riesgos involucrados y dentro de las limitaciones impuestas por el personal y los recursos físicos, tecnológicos, etc.

Las metas de un sistema seguro son :

- 1) Si un mensaje es aceptado por el sistema jamás será perdido, distorsionado, duplicado, acelerado, ni retrasado sin autorización.

- 2) El sistema jamás estará completamente fuera de servicio, aunque el servicio que ofrece ocasionalmente puede ser más bajo de lo normal.
- 3) La falla de un módulo o paso de transmisiones no aislará a ningún punto de la red de cualquier otro punto.
- 4) Cualquier error en la transmisión, recepción, formato de su contenido, o procesamiento de un mensaje será detectado y provocará la rápida notificación al personal de operaciones que es responsable del sistema.

El tema de la seguridad de los sistemas de comunicaciones de datos se puede analizar desde dos puntos de vista. El primero tiene que ver con los requerimientos que deben imponerse durante el diseño y la implantación del sistema, y el segundo tiene que ver con los requerimientos cotidianos de seguridad y confiabilidad necesarios para garantizar la operación segura del sistema.

3.2. REQUERIMIENTOS DE SEGURIDAD.

Para cada nivel de un sistema de comunicaciones es necesario considerar varios factores para obtener los niveles adecuados de seguridad.

Existen tres categorías básicas de requerimientos de seguridad en un ambiente de comunicaciones.

1) Prevención del acceso físico al lugar.- La precaución mas obvia que se puede tomar para establecer un ambiente seguro es la prevención del acceso no autorizado a la instalación o a los componentes del sistema. En el caso de los sistemas de comunicaciones, esto pudiera significar acceso a una terminal, a cualquiera de las líneas de comunicaciones y los puntos de intercambio de información, y al (los) centro(s) de cómputo y los archivos de datos. En el caso del centro de cómputo, la prevención seguiría los patrones normales que existen en cualquier ambiente restringido :

- a) Vigilancia.
- b) Cerraduras de puertas de tipo de identificación o de combinaciones.

Las medidas de seguridad requeridas para proteger los datos almacenados comienzan con la limitación del acceso físico a los medios de almacenamiento.

El acceso a las facilidades de transmisión es más difícil de evitar, debido a su propia naturaleza, quedan fuera del ambiente protegido de una terminal o de un centro de cómputo. Aún en las redes privadas arrendadas, las rutas de transmisión de mensajes pueden incluir líneas públicas durante alguna trayectoria, esto dá la posibilidad de la introducción sin permiso a los datos, por lo que es necesario contar con encriptores de software o hardware de tal forma que la información no sea legible.

2) Prevención del acceso operacional al sistema.- Si se logra el acceso físico a la instalación, el próximo nivel de seguridad tiene que ser la previsión del acceso operacional al sistema. Las características de seguridad a considerarse durante el diseño de la red de estaciones remotas, debería incluir :

- a) Control de las terminales.
- b) Estrictos procedimientos de "login" y "logout".
- c) Verificación de la identidad del operador en la consola de la computadora.
- d) Control de los mensajes de entrada y salida.

Si se logra el acceso a la computadora principal o al centro de control, el próximo nivel de seguridad es :

- a) La separación física del control de la computadora y el control de la red.
- b) Restricciones en cuanto a los tipos de datos que pueden enviarse o recibirse de los centros de control.

3) Protección contra la observación no autorizada.- Los dos propósitos principales de la observación de un sistema son la búsqueda de una o varias transacciones particulares y la recopilación de datos sobre la operación global, las estadísticas financieras, etc. La observación de las líneas con propósito de acumular datos "crudos", sería más difícil que su obtención por otros medios, por ejemplo, a través del personal que tenga acceso a los datos en su forma final y organizada.

La búsqueda de un mensaje específico es una razón viable para observar una línea. Aquí la protección está, bien sea en hacer que los datos sean inservibles en su formato observado o, en hacer que el uso del equipo de observación no sea económico.

3.3. CARACTERISTICAS DE SEGURIDAD RELACIONADAS CON EL MENSAJE

Muchos de los factores que influyen en las características de seguridad de las comunicaciones forman parte del diseño de los mensajes que pasan por el sistema.

1) Autorización de los mensajes.- Este proceso debe incluir las comprobaciones y aprobaciones necesarias, antes de que los mensajes entren al sistema. Para lograrlo se debe considerar lo siguiente :

- a) Validación de la terminal de origen respecto a si la estación correcta está dentro de la línea.
- b) Comprobación de que la estación está autorizada para transmitir en ese momento específico.
- c) Validación del formato del mensaje.
- d) Verificación de la autoridad del operador, para transmitir ese tipo de mensaje.
- e) Validación de la secuencia del número de mensaje.
- f) Prueba de los códigos correctos de autorización que se encuentran incorporados en el mensaje.

2) Validación de mensajes.- Cuando un originador autorizado ha dado entrada a un mensaje dentro del sistema, éste debe darnos la facilidad de :

- a) Editar las posiciones en cuanto a la corrección de los caracteres de control, campos de direccionamiento, datos, limitaciones de líneas y de formatos.
- b) Validar los datos en cuanto a números de enrutamiento, direcciones, tipo de códigos e información de contenido específico orientado respecto a un usuario determinado.

- c) Pruebas de autorización para los datos codificados, las palabras de prueba y otros tipos de prueba relacionados con la seguridad.

Una vez que el mensaje ha sido validado, se debe enviar un mensaje de aceptación positiva al originador.

3) : Entrega de mensajes.- El procedimiento de verificación es el siguiente :

- a) El destino es un punto válido dentro de la red.
- b) El destino está autorizado para recibir este tipo de mensaje.
- c) Se hace una conexión positiva con la estación y se le válida antes y después de la transmisión del mensaje
- d) Se recibe notificación de la aceptación del mensaje por parte del receptor, con la identificación de la terminal.
- e) Se transmiten números de salida continuos y seguidos como parte del mensaje.
- f) Se mantiene un registro histórico de todos los mensajes transmitidos.

4) Protección de los datos en los mensajes.- En el ambiente de comunicaciones existe muy poco sobre la protección contra la observación no autorizada de las líneas de las redes. Por lo tanto, para proporcionar el grado de seguridad necesaria para proteger los datos solo existe la encriptación de los mismos.

5) Contabilidad de los mensajes.- Una vez que el sistema ha aceptado un mensaje, se da por hecho que jamás se perderá o demorará por lo cual se contabiliza. Los datos que debe contener la contabilidad para facilitar el trabajo de auditoría deben ser :

- a) Estación de entrada y salida, identificación de la línea y número de secuencia.
- b) Fecha y hora de entrada.
- c) Cantidad de copias entregadas.

3.4. RECUPERACION DE UNA FALLA DEL SISTEMA

Existe la posibilidad de que el sistema total o varios de sus componentes fallen durante las operaciones normales. En las primeras etapas, las fallas probablemente se deberán a deficiencias del software (mal funcionamiento de los programas) o después de haberse hecho cambios a éste. Otras causas normales de las fallas son malos funcionamientos del hardware en las unidades principales o en los dispositivos periféricos. El sistema de recuperación debe tomar en consideración la contabilidad de los mensajes en tránsito bajo control del centro.

Se debe informar el estatus de todas las transacciones después de la recuperación.

Se requiere el almacenaje seguro de otros datos críticos para permitir el rápido y preciso retorno del sistema a estatus normal. Esto incluye la recuperación de los archivos de mensajes en tránsito, estatus de la red, estadísticas, resincronización de las líneas de comunicaciones, etc.

3.5. REQUERIMIENTOS OPERACIONALES PARA LA SEGURIDAD Y CONFIABILIDAD

La operación cotidiana del sistema dentro de un ambiente seguro y confiable, se puede lograr cuando se ha diseñado controles esenciales, procedimientos y respaldos. Suponiendo que existen todos los medios de control, el próximo paso es asegurar de que se usan en forma eficaz.

1) Seguridad operacional.- La eficacia de un programa de seguridad reside en la provisión de protección a un nivel realista y alcanzable. Las medidas de control, que son demasiado estrictas, no se seguirán, y este descuido rápidamente se propagará a las demás precauciones de seguridad. Por lo tanto, la meta principal debería ser la de lograr un nivel de control que pueda ejercerse y luego, observarlo con rigidez. Esto incluye, el uso y la comprobación de pase de identificación, cerrar con llave los archivos y guardar las contraseñas y códigos.

Deberán programarse simulacros de incendio y el personal deberá mantener al día sobre los nuevos procedimientos de emergencias.

Los mecanismos de seguridad tales como las cerraduras automáticas para las puertas, deberán estar en buen funcionamiento en todo momento.

El control de la documentación del sistema es tan importante como el control del equipo. Las listas y especificaciones detalladas de los programas, al igual que los libros de código y los manuales de operaciones deberán guardarse bajo llave cuando no están en uso.

- 2) **Confiabilidad operacional.**- El control del uso, la programación y la observación de los programas diarios y periódicos de mantenimiento, son los factores principales para garantizar la confiabilidad del sistema. Otros factores de confiabilidad, se basan en el mantenimiento del equipo.

El personal de operaciones debería asegurarse de que existan unidades de repuesto en posición, o un extenso inventario de piezas de repuesto en algún depósito apartado, particularmente si el sistema está muy cargado. También deberán ser responsables de llevar al cabo frecuentes pruebas de ejecución del sistema, de utilización, de tiempo muerto y de recuperación, al igual que vigilar la entrada de energía eléctrica y las condiciones ambientales tales como la temperatura y la humedad. Los programas de mantenimiento y el inventario de piezas para las ubicaciones remotas tienen que estar listos y disponibles cuando hagan falta. El equipo de pruebas que se necesita para el mantenimiento es muy importante por lo que debe ser utilizado únicamente por el personal indicado.

- 3) **Control de tráfico y mensajes.**- El área final de un programa de seguridad de las operaciones cotidianas tienen que ver con el control de tráfico y los mensajes. Esto abarca todos los aspectos de la retención de los archivos, áreas de recuperación y la limpieza interna del sistema.

Un procedimiento que debería ejecutarse diariamente involucra el rastreo de todos los archivos de mensajes activos para encontrar tráfico que no haya sido entregado. Aunque es posible que alguno de estos mensajes se hayan diferido intencionalmente en su entrega posterior, puede haber otros mensajes que permanecieran en el sistema inadvertidamente. Esto pudiera deberse a problemas de software o de hardware.

En el área de control de los mensajes, todos los errores de los mensajes deberían reconciliarse diariamente al igual que las cifras de entrega de tráfico según los mensajes enviados y recibidos. El uso de programas de reconciliación fuera de línea para rastrear los registros de los mensajes y balances del tráfico recibido contra el entregado, es una ayuda valiosa en esta tarea.

Para cumplir con los niveles de seguridad mencionados, a continuación se encuentra un conjunto de cuestionamientos que evalúan los niveles de seguridad :

3.6. DEFINICION DE UN SISTEMA DE TELECOMUNICACIONES SEGURO.

3.6.1. SEGURIDAD ADMINISTRATIVA

Se evaluarán los procedimientos de control a los usuarios y administradores de la red y se realizarán pruebas para confirmar qué tan estandar y eficaz son los procedimientos de seguridad.

¿ Quien es responsable de la seguridad de la red ?
(persona, departamento, organización)

¿ Qué funciones realiza ?

- Decir qué procedimientos utiliza para verificar la seguridad de la red
 - ¿ Con qué frecuencia se verifica ?
 - ¿ A quién reporta los resultados ?
- ¿ Qué seguimiento se le dá a los resultados ?

Evaluar dichas funciones, con objeto de conocer su eficiencia.

Conocer qué tan efectiva y confiable es la seguridad en las regiones, zonas y plazas. Si no es así, ¿Cuál es el motivo ?

Proponer forma de estandarización.

¿ Existe un estándar en los procedimientos de seguridad en las regiones ?

¿ Existe algún tipo de administración de cambios que permite control de alteraciones a las configuraciones de software o hardware ?

¿ Qué área lo realiza ?

¿ Cuáles son las funciones de esa área ?

Documentación de fallas de seguridad.

¿ Cuáles son las fallas más comunes ?

¿ Cómo se documentan los problemas de seguridad ?

¿ Quién conoce estos problemas ?

¿ Qué seguimiento se les dá ?

3.6.2. SEGURIDAD EN SOFTWARE

Se evaluará la eficacia del software con que se cuenta, tanto para la seguridad de la información como para la administración de claves de acceso a la red, además, se revisarán las medidas que existen para proteger el software que es crítico para la operación de la red de comunicaciones, contra la manipulación o destrucción no autorizada, finalmente se verán los niveles de protección que existen para el uso de las facilidades que ofrece la computadora para acceder la red de comunicaciones.

Evaluar el software para la seguridad de la información.

¿ Se cuenta con un software para la seguridad de la información ?

¿ Este software cumple con los requerimientos de seguridad del banco ?

¿ Están las políticas de seguridad en función del software y hardware que se tiene ?

¿ Cuando se realiza un cambio en la estructura de comunicaciones (equipo), cambian estas políticas ?

¿ Quién documenta estos cambios ?

¿ Esta la organización del departamento soportando la seguridad de software y hardware ?

Definir la forma de administración de claves de acceso. Evaluar el software de verificación de claves.

¿ Quién administra las claves de acceso ?

¿ Cómo las administra ?

¿ Se realiza la validación de password ?

¿ Cuántas veces permite intentar el password ?

- ¿ Cómo se le dá mantenimiento al archivo de password ?
- ¿ Qué políticas existen para la asignación de password ?
- ¿ Cómo se distribuyen los password ?
- ¿ Quién los distribuye y dá mantenimiento ?
- ¿ Se cambia con frecuencia los password y los dispositivos de protección ?
- ¿ Están todas las terminales que accesan la red claramente identificadas ?
- ¿ Existen controles de ruteo para evitar que los usuarios especifiquen sus rutas de acceso ?
- ¿ Con qué frecuencia se verifica la existencia de estos controles ?
- ¿ Cómo se limita el número de intentos para conectarse a la red ?
- ¿ Cómo se registran estos intentos ?
- ¿ Cómo se monitorean ?
- ¿ Qué procesos se ejecutan en la red con fines de auditoría ?
- ¿ Cómo se registran los accesos y/o actividades no autorizadas ?

3.6.3. SEGURIDAD EN HARDWARE

Se evaluará el hardware que se tiene para la seguridad de la información en el momento de la transmisión, además, se realizará el estudio de los métodos de estudio de encriptación de datos.

Evaluación de la encriptación de los datos :

- ¿ Con qué hardware se cuenta para la seguridad de la red ?
(equipo : para verificar claves, encriptar, etc).

Revisar el hardware para verificación de claves.

Revisar el método de encriptación de claves.

Verificar el funcionamiento de los encriptores.

Evaluar método de encriptación para todos los diferentes tipos de encriptores que se tengan.

¿ Con qué frecuencia se dá mantenimiento a este equipo ?

¿ Quién dá el mantenimiento ?

¿ Se realizan pruebas a los encriptores para prever fallas ?

¿ Existe un responsable del funcionamiento de los encriptores ?

¿ Se cuenta con una bitácora de utilización ?

¿Cuál es el funcionamiento de los encriptores ?

3.6.4. PLANES DE CONTINGENCIA

Se evaluarán los planes de recuperación, en caso de que se presente cualquier tipo de contingencia, midiendo en la red el alcance de recuperación de todas aquellas aplicaciones que transmiten datos que son críticos para la operación de la Institución, así como la evaluación de las pruebas que se hayan realizado a los procedimientos de recuperación de desastres.

Asimismo, se considerarán también los dos aspectos importantes dentro de los planes de recuperación: el primero, la evaluación y el grado de eficacia que tienen dichos planes, el segundo, se evalúan los niveles de responsabilidad que se tienen asignados para la ejecución de los procedimientos que se aplican en el caso de que se presente una contingencia.

Finalmente, la identificación de las amenazas y riesgos significativos que puedan impactar en la red de comunicaciones.

Evaluar los planes de contingencia

¿ Es el edificio del centro de comunicaciones sólido en su estructura ?

Está protegido contra :

Huracanes
Daños por inundación
Terremotos

¿ Se cuenta con un seguro para edificios, instalaciones y equipo ?

¿ Cuáles son las características de los seguros ?

¿ Está el edificio y el equipo correctamente conectado a tierra como medida de protección contra rayos ?

¿ Con qué enlaces alternos se cuenta ?

¿ Se ha realizado alguna evaluación del nivel de riesgo y amenazas probables a la red ?

Describir los planes de contingencia con que se cuenta.

¿Cuál es el alcance de recuperación ?

¿ Qué sucede con la transmisión de datos críticos para la operación del Banco ?

¿ Se han realizado pruebas a los procedimientos de recuperación de desastres ?

¿ Se ha evaluado la eficiencia que tienen dichos planes ?

¿ Quién desarrollaría estos planes ?

¿ Está capacitado el personal para esta situación ?

¿ Cómo se lleva al cabo esta capacitación ?

¿ Se ha requerido un plan de contingencia ?

¿ Se cuenta con un directorio del personal responsable de una contingencia ?

¿ Quién fija prioridades en una contingencia ?

¿ Cuáles son las prioridades ?

3.6.5. SEGURIDAD FISICA

Revisar la seguridad de las instalaciones del área de comunicaciones, así como el acceso a las mismas.

Controles de Fuego

¿ Está el área de comunicaciones ubicado en un edificio resistente al fuego ?

¿ Está la sala del equipo separada de las áreas adyacentes mediante particiones, paredes, pisos, y puertas resistentes al fuego y separados de contenidos peligrosos ?

¿ Están hechos los pisos y techos a prueba de incendios ?

¿ Se guarda el papel y otros suministros combustibles fuera del área del equipo ?

¿ Está prohibido fumar en el área de equipo ?

¿ Está el personal operativo adiestrado en técnicas de extinción de incendios, y tienen responsabilidades individuales asignadas para estos casos ?

¿ Está el centro de cómputo protegido con sistemas de extinción automáticos ?

- Agua,(en este caso suena una alarma).
- Dióxido de carbono

¿ Hay extintores de fuego portátiles ubicados estratégicamente en el centro. (ubicación visible) ?

¿ Están los controles de emergencia para desconectar la energía eléctrica, accesibles en las salidas ?

¿ El control de emergencia interrumpe : energía eléctrica, calefacción, ventilación y aire acondicionado ?

¿ Se usa una lista de comprobación para apagar el equipo ?

Hay detectores de humo y de ionización instalados en:

- a) ¿ Varias zonas del centro de cómputo ?
- b) ¿ Techos ?
- c) ¿ Suelos falsos ?
- d) ¿ Conductores de ventilación ?

¿ Se hacen pruebas regulares de los detectores ?

¿ Se hacen ejercicios de simulación de incendios con regularidad ?

¿ Hay una cantidad suficiente de cajillas de alarma de incendios en el área ?

Al activarse la alarma de incendios, suena :

- a) ¿ Localmente ?
- b) ¿ En el puesto del guardia de seguridad ?
- c) ¿ En una estación central de alarmas de incendios ?

¿ Se usan materiales flamables en el mantenimiento del equipo ?

¿ Hay suficiente suministro de iluminación de emergencia por todo el centro de cómputo ?

Controles De Agua

¿ Está el equipo arriba del nivel del suelo ?

¿ Están las tuberías de agua que pasan por arriba, fuera de la sala del equipo, con excepción de surtidores de emergencia ?

¿ Hay un drenaje adecuado en el piso de encima para evitar que se filtre el agua por el techo ?

¿ Se proporciona un drenaje adecuado en las áreas adyacentes al centro de cómputo ?

¿ Están hechas las puertas y ventanas a prueba de agua ?

¿ Se ha proporcionado protección contra agua (lluvia) acumulada o contra goteras en el tejado y en las torres de enfriamiento que están sobre el tejado ?

Controles De Electricidad

¿ Es el suministro eléctrico local confiable ?

¿ Está el voltaje de las líneas registrado con un voltímetro que muestra los voltios que pasan ?

Si el voltaje de la línea no es confiable, ¿ Se han investigado medidas alternas ?

¿ Se atienden todos los cables eléctricos del centro de cómputo con lo estándares de códigos eléctricos ?

Controles De Acceso

¿ Es el centro de comunicaciones un objetivo poco probable para delincuentes ?

¿ Hay guardias de vigilancia en todas las entradas del centro ?

¿ Se exige una constancia de identificación para entrar a las instalaciones ?

¿ Está el acceso al centro restringido solamente a las personas autorizadas, por ser este su lugar de trabajo ?

¿ Está el acceso a las instalaciones restringido las 24 hrs. ?

¿ Se usan llaves, cerraduras de códigos, u otros dispositivos de seguridad para controlar el acceso ?

¿ Es necesaria cada una de las entradas al centro de cómputo ?

¿ Están las salidas de emergencia protegidas con alarmas ?

Si el acceso al centro de cómputo se controla eléctricamente, ¿hay energía eléctrica de baterías cerca y disponible durante las interrupciones eléctricas?

Controles De Aseo y Mantenimiento

- ¿ Se evita la acumulación de escombros en el centro de cómputo ?
- ¿ Se limpia con regularidad el equipo y las superficies de trabajo ?
- ¿ Se lavan los pisos con regularidad ?
- ¿ Se limpian con regularidad las superficies que están debajo de los pisos falsos ?
- ¿ Se vacían los recipientes de basura fuera del área, para disminuir la descarga de polvo ?
- ¿ Se prohíbe comer en la sala del equipo ?

Controles Asuntos Generales

- ¿ Se ha orientado al personal de seguridad y de operaciones de cómo se debe reaccionar en caso de disturbios civiles ?
- ¿ Se ha adiestrado al personal de cómo manejar amenazas de bombas ?
- ¿ Hay un programa de enlace con las agencias locales de orden público ?

3.6.6. SEGURIDAD EN LA TRANSMISION

Se analizarán los protocolos utilizados en la transmisión de datos.

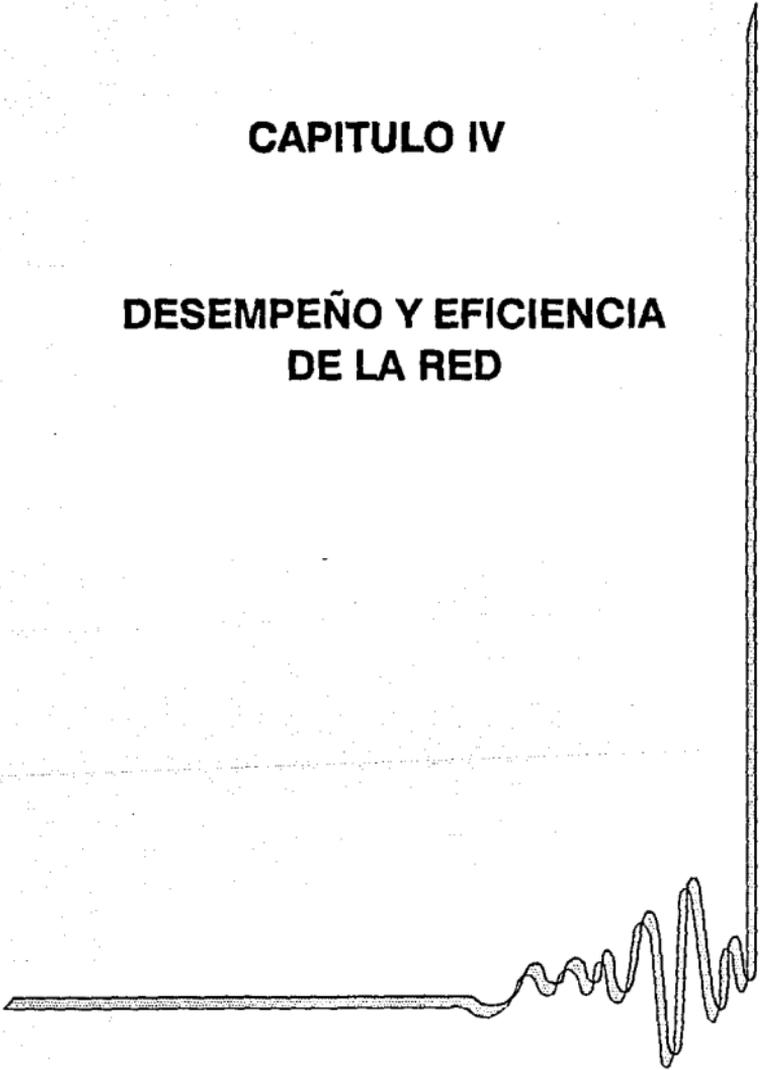
- ¿ Cuáles son los protocolos que se utilizan ?

Solicitar diagrama de conexión de equipos mencionando los protocolos que se utilizan.

Evaluar la seguridad y control que ofrece cada uno de los protocolos.

CAPITULO IV

DESEMPEÑO Y EFICIENCIA DE LA RED



CAPITULO IV

DESEMPEÑO Y EFICIENCIA DE LA RED

En este capítulo evaluaremos el desempeño y eficiencia de la red de telecomunicaciones, lo que depende de un análisis a los parámetros que se consideran y la forma en que se desarrolla la medición de los mismos, por lo que iniciaremos definiendo la forma en que nosotros realizaremos las mediciones.

Un método es "Prueba selectiva de auditoría". Esta prueba en una auditoría es un método por el cual se obtienen conclusiones sobre las características de un conjunto de eventos mediante el examen de un grupo parcial de ellos (muestra).

Ahora la pregunta es ¿ Cuántas muestras representativas del área o rubro sujeto a revisión serán necesarios para un buen trabajo de auditoría ?

4.1. CONCEPTOS BASICOS DE MUESTREO

Para esto definiremos algunos conceptos estadísticos.

Censo es medir o contar hechos (sucesos) que forman un grupo (universo). En los casos que no es posible medir o contar las unidades se puede proceder seleccionando algunos de los ejemplares del universo y hacer con ellos observaciones que puedan ser aproximadas a las que se hicieran si se revisara totalmente el universo o población del que forman parte. Este procedimiento recibe el nombre de muestreo y la unidad seleccionada se llama muestra. En la muestra deben de estar representadas las diferentes magnitudes, características y condiciones de la población de la que fue extraída.

Es importante destacar que entre más elementos de prueba se tengan, se tendrán más elementos de juicio para expresar su opinión. Además es necesario verificar el costo que produce una auditoría exhaustiva contra los resultados esperados.

Para todo esto se han desarrollado métodos para seleccionar las muestras de auditoría y valiosos planes de muestreo estadístico que ayudan al auditor a desarrollar un buen trabajo.

4.2. METODOS DE MUESTREO

Existen dos métodos los cuales se usarán dependiendo de la práctica, criterio, conocimientos, juicio y sobre todo de los resultados que espera de su trabajo.

- 1) Muestreo de criterio.
- 2) Muestreo estadístico.

Existe la posibilidad de que se realice un muestreo con la combinación de ambos.

Puede darse el caso de que en un universo dado existan diferencias entre los elementos que lo conforman, por lo que resulta conveniente hacer una segregación agrupando por conceptos, características físicas o especiales, o por los valores implícitos en cada uno de los componentes del universo. Este procedimiento se denomina estratificación de población. Una vez conformados los estratos, se procederá a muestrear separadamente cada uno de ellos y los resultados obtenidos se pueden reunir para obtener una imagen completa del universo, o bien, considerarse por separado atendiendo a los objetivos que se persiguen en la revisión.

Cada estrato se muestreará dependiendo de las características que requiera la auditoría.

En el Anexo 3 se definen los métodos de muestreo de criterio con su selección de muestras (Selección a juicio del auditor, por intervalos, por bloques o conglomerados, y por números aleatorios); y el método estadístico (muestreo por atributos y por variables).

A continuación se encuentran los aspectos que se deben cubrir para realizar una evaluación del desempeño y eficiencia.

4.3. ASPECTOS A EVALUAR DEL DESEMPEÑO :

- Disponibilidad
- Capacidad máxima de transmisión
- Tiempo de respuesta para transacciones interactivas.
- Utilización de la red.

Objetivo determinar los parámetros que se utilizan para evaluar el desempeño de las telecomunicaciones en el banco.

¿ Quién define estos parámetros ?

¿ Cómo se lleva a cabo la selección de parámetros ?

¿ Quién evalúa que dichos parámetros son los correctos para medir el desempeño de la red ?

¿ Cómo se evalúan estos parámetros para identificar condiciones anormales o problemáticas ?

¿ Cómo se define que una situación es crítica o no ?

En qué se basa la definición de parámetros y metas de desempeño :

- Objetivos del negocio
- Características de la tecnología
- Requerimientos operativos, etc.
- Otros

Analizar que los parámetros utilizados sean los adecuados para obtener los resultados esperados.

¿ Porqué son los adecuados ó inadecuados ?

Definir los parámetros de desempeño que reflejan la calidad del servicio desde el punto de vista cliente.

- Tiempos de espera causados por la red.
- Confiabilidad de las transacciones.
- Otros.

Realizar la verificación de dichos parámetros.

¿ La institución considera válido este tipo de parámetros ?

Evaluar el proceso de medición

¿ Cómo se seleccionan las muestras (describir método)?

¿ Se actualizan las muestras a medida que cambian las condiciones operativas ?

¿ Cómo se efectúan las mediciones de desempeño ?

- Manualmente
- Equipo aislado de prueba
- Sistemas de medición automático.

Se realiza validación y ajuste a los sistemas de medición en forma periódica.

Las mediciones actuales permiten distinguir los componentes principales que afectan el desempeño.

- Computadoras
- Procesador Front End
- Controlador remoto de terminales
- Modems y multiplexores
- Canales de transmisión
- Errores humanos
- Equipos terminales
- Otros

Evaluar método(s) estadístico(s) utilizado(s)

¿Cuál es el método estadístico utilizado ?

¿ Comprobar la forma en que se utiliza ?

¿Cuál es el componente que afecta más el desempeño de la red ?

¿Cuál es la causa principal ?

¿ Existe alguna persona que se encargue de mejorar el desempeño de la red ?

¿Cuál es su puesto y qué funciones desempeña ?

Revisión de los reportes de desempeño generados

¿ Qué reportes se emiten sobre el desempeño ?

¿ Con qué frecuencia ?

¿Cuál es su distribución ?

¿ En la realidad se utilizan dichos reportes ?

¿ Algún área de auditoría recibe estos reportes ?

¿ Cómo se resuelven los problemas de desempeño ?

¿ Quiénes son los encargados y por qué ?

¿ La misma área de comunicaciones resuelve estos problemas o los asigna a otra área ?

4.4. ASPECTOS A EVALUAR DE LA EFICIENCIA

Costo promedio por transacción.

¿ Cual es el método utilizado ?

¿ Cómo se mide el aprovechamiento (utilización) de los equipos ?

Definir los parámetros de eficiencia y productividad que son relevantes a la operación de las redes.

¿ Cuáles son los parámetros que se consideran ?

¿ Cuáles se miden actualmente ?

¿ Qué parámetros se consideran para las mediciones ?

¿ Cómo se miden ?

¿ Cuáles son las metas de productividad y eficiencia que existen en el banco ?

Se hace uso de herramientas de optimización de recursos de telecomunicaciones para :

Reconfiguración óptima de la red a medida que cambian los requerimientos de operación.

Evaluación periódica de alternativas tecnológicas, nuevos productos/servicios y proveedores alternos.

Decisiones compra vs alquiler de equipos.

¿ Quién realiza estas funciones ?

Evaluación de los reportes generados sobre eficiencia

¿ Qué reportes sobre eficiencia y productividad se emiten actualmente ?

¿Cuál es su distribución ?

¿ Qué utilización tienen ?

¿ Qué seguimiento se les da ?

¿ Recibe el área de auditoría copia de estos reportes ?

¿ Ha existido alguna variedad en la eficiencia, en función a qué se presenta ?

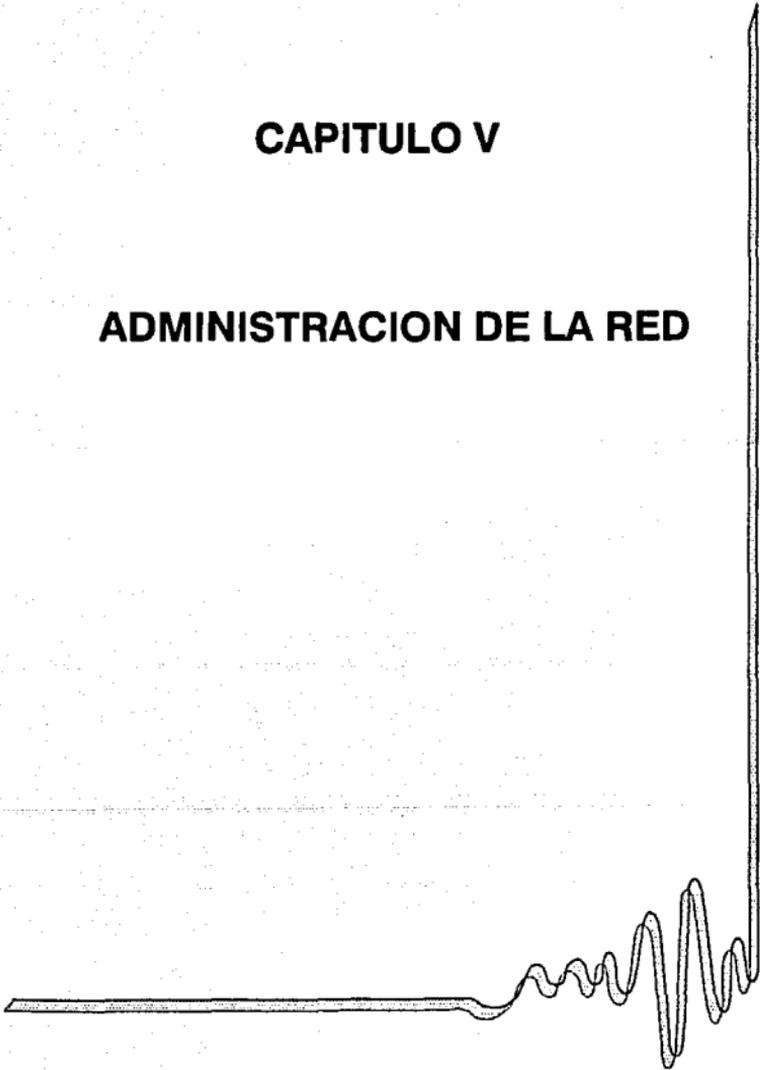
¿ Cómo se realiza el proceso de selección de proveedores y adquisición de equipos y servicios de telecomunicaciones ?

¿ Qué área realiza estas funciones ?

¿ Qué criterios de eficiencia o productividad se incorporan en la evaluación de proyectos ?

CAPITULO V

ADMINISTRACION DE LA RED



CAPITULO V

En este capítulo analizaremos los aspectos relacionados con la administración de la red y sus posibles requerimientos futuros. El primero consiste en los aspectos de monitoreo, fallas, mantenimiento de equipo, organización y funciones del área. El segundo, la planeación (corto, mediano y largo plazo), compras de equipo e integración de equipo.

Es importante destacar que en la parte de administración de la red se encuentran relacionados todos los puntos anteriores de estudio, ya que sin una buena administración no se puede tener seguridad, desempeño, eficiencia y control en una red en forma adecuada.

Para la administración de la red y planeación de requerimientos futuros. es necesario conocer las diferentes etapas de la administración, estas son: planeación, organización, integración, dirección y control

Proceso	Planeación
Administrativo	Organización
	Integración
	Dirección
	Control

(*)

Planeación. La planeación consiste en fijar el curso concreto de acción que ha de seguirse, estableciendo los principios que habrán de orientarlo, la secuencia de operaciones para realizarlo y las determinaciones de tiempos y de número, necesarias para su realización.

Organización. Organización es la estructura técnica de las relaciones que deben existir entre las funciones, niveles y actividades de los elementos materiales y humanos de un organismo social, con el fin de lograr su máxima eficiencia dentro de los planes y objetivos señalados.

(*)

Definición de Agustín Reyes Ponce (Administración de Empresas, editorial Limusa, S.A. de C.V. 1968).

Integración. Integrar es obtener y articular los elementos materiales y humanos que la organización y la planeación señalan como necesarios para el adecuado funcionamiento de un organismo social. La planeación nos ha dicho "que" debe hacerse, y "cuando"; la organización nos ha señalado quiénes, dónde y cómo deben realizarlo. Falta todavía obtener los elementos materiales y humanos que llenen los cuadros teóricos formados por la planeación y la organización; esto lo hace la integración.

Dirección. La dirección es aquel elemento de la administración en el que se logra la realización efectiva de todo lo planeado, por medio de la autoridad del administrador, ejercida con base en decisiones, ya sea tomadas directamente o delegando dicha autoridad, y se lleva simultáneamente que se cumplan en la forma adecuada todas las órdenes emitidas.

Control. Es la medición de los resultados actuales y pasados, en relación con los esperados, ya sea total o parcialmente, con el fin de corregir, mejorar y formular nuevos planes.

5.1. ASPECTOS A EVALUAR DE LA ADMINISTRACION DE LA RED.

- Administración de Fallas
- Administración de Desempeño
- Administración de Configuración
- Administración de Servicios
- Revisión a la organización y funciones del área

Para esta parte tomaremos en cuenta dos acciones:

Definir qué sistemas de administración y control de la red se encuentran implantados.

Los sistemas actuales de administración responden a los requerimientos de medición y control de seguridad, desempeño y eficiencia establecidos en el la Institución.

Para lograr lo anterior es necesario que el auditor pueda contestarse las siguientes preguntas :

- ¿ Qué sistemas se tienen para monitorear la red ?
- ¿ Se cuenta con un equipo exclusivo para monitorear la red ?
- ¿ Características principales de monitoreo ?
- ¿ A qué niveles se puede monitorear ?
- ¿ Cómo se detecta una falla ?
- ¿ Cómo se clasifican las fallas ?
- ¿ Existen prioridades en corrección de fallas ?
- ¿ Quién les da seguimiento ?
- ¿Cuál es el puesto de esta persona y qué funciones desempeña ?
- ¿ Se realizan diagnósticos (pruebas) para prever fallas ?
- ¿ Cómo se realizan dichas pruebas ?
- ¿ Cómo se almacena la información ?
- ¿ Se lleva en forma manual o automática ?
- ¿ Qué políticas existen para el almacenamiento de información ?
- ¿ En el sistema de monitoreo se identifica claramente el desempeño de la red ?
- ¿Cuál es la forma de identificar un usuario ?
- ¿ Se han tenido problemas al tratar de identificar un usuario ?

Existe una estrategia para la administración de la red que :

- Plantee una visión de cómo evolucionaría la arquitectura de control con los avances tecnológicos.
- Defina las interfaces clave entre sistemas actualmente aislados, como también el nivel adecuado de integración.

¿Cuál es la forma de controlar los servicios de comunicaciones solicitados ?

¿ Cómo clasifican a sus usuarios ?

¿ Con frecuencia el área desarrolla funciones que no tiene establecidas ?

¿ El departamento se encuentra organizado por áreas funcionales ?

¿ Las funciones actuales están de acuerdo con su organigrama?

¿ Qué funciones realizan los empleados para cubrir un puesto temporalmente vacante (falta de personal) ?

¿ Se cubre una vacante hasta que se llega a una situación crítica ?

¿Cuál es la antigüedad de las personas que dirigen el área ?

¿ Existe definido un método para comunicación formal entre las áreas de operación y las administrativas de esta área ?

¿ Existen reuniones periódicas (juntas de trabajo) para exponer opiniones de área ?

¿ Se da copia de la minuta a todos los asistentes ?

¿ Se obtiene un beneficio de las reuniones ?

¿ Se tienen por escrito políticas y procedimientos del área ?

¿ Las políticas y procedimientos comprenden la seguridad y control del área ?

¿ Los empleados nuevos tienen un entrenamiento especial antes de iniciar labores ?

¿ Se realiza esta capacitación formalmente ?

El entrenamiento incluye :

- Procedimientos de emergencia
- Seguridad
- Formalidad en el área de trabajo
- Confidencialidad del trabajo que se desarrolla.

¿ Se recoge todo tipo de llaves, credenciales, etc., Cuando un empleado deja definitivamente el área ?

¿ El tipo de entrenamiento incluye la parte técnica y administrativa ?

¿ En el plan de actividades anual se incluye tiempo para capacitación ?

¿ En la descripción de actividades se han formalizado los puntos donde se necesita una autorización ?

En la descripción de actividades se incluye :

- El puesto que se ocupa
- Las responsabilidades del puesto
- El puesto del responsable al que se reporta

¿ Se compensa a todos los empleados por tiempo extra?

¿ El gerente analiza las causas de requerir tiempo extra (se incluye falta de enlaces, días pico, etc)?

¿ Cómo se controlan las vacaciones de los empleados?

¿ Existen políticas para la promoción interna ?

¿ Se evalúa periódicamente a los empleados ?

¿ conocen los empleados su evaluación ?

¿ Existen reportes que contengan la información sobre problemas de operación y eficiencia del equipo utilizado ?

¿ Existe un archivo actualizado de proveedores ?

- Empresa
- Nombre vendedor
- Teléfono
- Actividad
- Descripción del producto o servicio
- Fecha de adquisición
- Expedición de contrato
- Importes.

¿ Qué políticas y procedimientos se han establecido para dar mantenimiento ?

¿ Cómo se lleva el control de los contratos de mantenimiento?

Enunciar los tipos de contratos de mantenimiento que se tienen.

¿Cuál es la frecuencia de cada uno ?

¿ Con base en qué definen la frecuencia ?

¿ Qué sucede al vencimiento de los contratos ?

¿ Quién administra estos contratos ?

¿ Los contratos antes de firmarse son revisados por un área especial ?

Los contratos tienen cláusulas como :

- En caso de pérdida (total o parcial)
- Pérdidas en la empresa por retraso de entrega
- Crédito
- Patente (derechos de propiedad)
- ¿ Qué sucede si se cancela el contrato ?

¿ Existen contratos para todos los servicios (dados y recibidos) ?

¿ Existe un procedimiento formal para evaluar los contratos ?

¿ Se cuenta con seguro para el equipo ?

¿ Se tiene un control donde se indique qué empleados tienen acceso al equipo ?

¿ Se diferencian las claves de la gente que realiza mantenimiento o modificaciones ?

¿ Existe un plan de capacitación formal para el uso del equipo ?

¿ Existen políticas internas del uso del equipo ?

5.2. EVALUACION DE REQUERIMIENTOS FUTUROS

Como objetivo de esa parte identificaremos los requerimientos futuros de telecomunicaciones como son :

- Necesidades de integración
- Crecimiento esperado de tráfico
- Simulación de trafico esperado
- Desarrollo futuro de la banca electrónica
- Procesos de simulación en la red

con la finalidad de poder evaluar su impacto en las necesidades de auditoría (seguridad, desempeño, eficiencia, y administración de la red).

De la misma foma que el punto anterior se necesita que el auditor conozca la respuesta de las siguientes preuntas :

¿ Existe un plan maestro para la red de comunicaciones ?

¿ Cuántos años incluyen el plan ?

¿ Estos planes se basan en los institucionales ?

¿ Se consideran avances tecnológicos en los planes ?

¿ Se proyectan los requerimientos de hardware, software y personal ?

¿ Existen fechas en el plan de actividades ?

¿ Existe un procedimiento formal para actualizar los planes de trabajo?

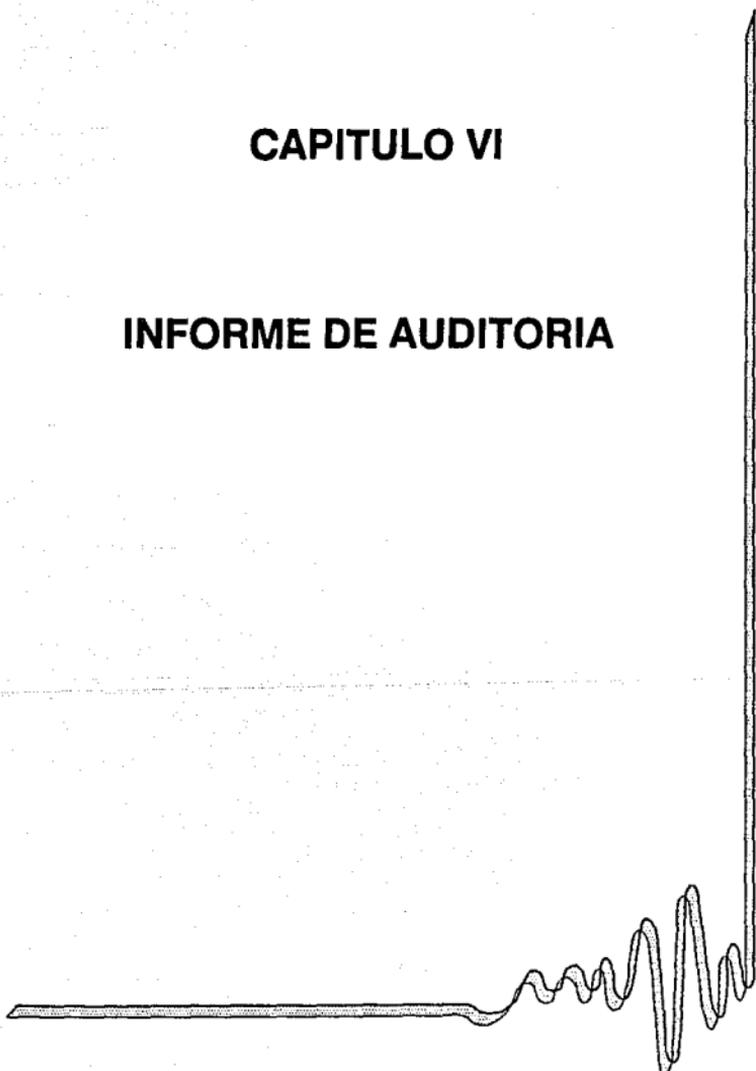
¿ Existe un comité que se encargue de ver las funciones de planeación ?

¿ Quién forma el comité ?

- ¿ Participa o se entera auditoría del comité ?
- ¿ Existen minutas de las reuniones de comité ?
- ¿ Todos los participantes tienen copia de las minutas?
- ¿ Se tiene planeado hacer la compra de equipo?
- ¿ Cómo se define la adquisición de equipo ?
- ¿ Quién define la necesidad de equipo ?
- ¿ Quién autoriza la adquisición de equipo ?
- ¿ Hay procedimientos escritos para desarrollo y mantenimiento de los estándares de comunicaciones ?
- ¿ Existe un grupo específico de personas para desarrollo de estándares?
- ¿ Existe un plan para la implantación de los estándares ?
- ¿ Cómo y quién autoriza los estándares ?
- ¿ Existe un manual de estándares ?
- ¿ Se distribuye a las áreas involucradas ?
- ¿ Las autoridades realizan acciones para corregir situaciones que no van de acuerdo con los estándares?

CAPITULO VI

INFORME DE AUDITORIA



CAPITULO VI

INFORME DE AUDITORIA

Sin lugar a dudas, una de las fases más difíciles y determinantes en el trabajo de auditoría es la elaboración del informe final, ya que son muchos los factores que inciden en esta actividad y que el auditor debe tomar en cuenta para concluir con su revisión.

Una buena auditoría con un mal informe podría ser la causa de no ser considerada en su totalidad.

6.1. ELEMENTOS BASICOS DEL INFORME

Como primer paso a dar, previo a la preparación de un informe será determinar quién o quienes serán los lectores del documento, es decir, considerar que lo puede leer la autoridad más alta de la organización, así como el personal de menor rango del área auditada.

Por lo anterior es recomendable que el informe considere dos presentaciones : una de resumen que sintetice los resultados o hallazgos más importantes producto de la auditoría, y otra presentación detallada con toda la información necesaria que formalice el trabajo realizado.

La información detallada deberá contener los siguientes elementos :

- **Introducción.** Dirigida al lector del informe refiriéndose a los objetivos o instrucciones que se le giraron al auditor para dar efecto a su trabajo.
- **Alcance de la revisión.** Por alcance se entenderá la profundidad aplicada en las investigaciones, las áreas que se han examinado y evaluado, una breve descripción de las técnicas y procedimientos de auditoría que se emplearon, el plan de muestreo o método de selección de muestras elegido, y referencia a los auditores o especialistas que intervinieron en el trabajo.
- **Limitaciones.** Es común que durante el desarrollo de la auditoría se le presenten al auditor situaciones que le impiden ejercer su labor en forma normal, como son : falta de cooperación del personal de la entidad auditada, información poco confiable, etc.

- **Resultados.** En esta sección se detallarán los resultados del trabajo realizado y los hallazgos de auditoría, cuidando de dejar perfectamente claro y soportado todas y cada una de las aseveraciones que se presenten. El soporte puede manejarse por medio de anexos al informe.
- **Sugerencias.** Se presentarán las sugerencias que se juzgue pertinentes y que estén en congruencia con los resultados y hallazgos reportados en la sección anteriormente descrita.
- **Cierre del informe.** Parte final del informe que indica el lugar y la fecha en que se emitió y el nombre y firma del responsable del contenido del informe, quien generalmente es la misma persona que está a cargo del grupo de auditoría.

6.2. CARACTERISTICAS DE UN INFORME

La información que proporcione el reporte de auditoría acerca de los actos, hechos o situaciones observadas, deben reunir los siguientes atributos de calidad.

- **Oportunidad.** De tal manera que la información permita tomar a tiempo las acciones requeridas.
- **Integridad.** Deben incluirse todos los hechos importantes observados, sin omisión alguna, proporcionando una visión objetiva de las cuestiones advertidas y de las conclusiones y recomendaciones a que conducen.
- **Competencia.** Asegurarse de que los resultados informados corresponden al objeto de la auditoría.
- **Relevancia.** Considerar los asuntos trascendentes para la situación u operación de las áreas examinadas, sin abundar en los detalles innecesarios.
- **Objetividad.** Presentar con imparcialidad la verdad o realidad de los actos, hechos o situaciones comprobados, hasta donde dicha verdad o realidad sean razonables y estén respaldados con evidencia probatoria.
- **Convicción.** Hacer que la solidez de la evidencia conduzca a cualquier persona prudente a las mismas conclusiones a que llego el auditor.

- Claridad. Cuidar que la estructura, terminología y redacción empleadas, permitan que la información presentada pueda ser entendida por cualquier persona, aún la no versada en el tema.
- Utilidad. Apoyar elementos que propicien la optimización del uso de los recursos y el mejoramiento de la administración de la dependencia o entidad.

6.3. DISCUSION DE LAS CONCLUSIONES Y RECOMENDACIONES CON LOS RESPONSABLES DE LAS AREAS AUDITADAS

Salvo casos de excepción, debidos a la naturaleza de la investigación o a la índole de las observaciones encontradas, como la presunción de actos indebidos, el auditor discutirá su informe con los responsables de las áreas examinadas, antes de su presentación formal. En esa discusión podrá conseguir pruebas adicionales y elementos de juicio que no se le hayan aportado durante el desarrollo de su trabajo y lo lleven a modificar su opinión y en todo caso le permitirá asegurar en lo posible la solidez de la evidencia obtenida, la validez de sus conclusiones, la pertinencia de las recomendaciones y la objetividad e imparcialidad de su informe.

Si hay desacuerdo entre los responsables de las áreas examinadas y el auditor, éste solicitará que se le presenten por escrito los puntos de vista contrarios, debidamente razonados, los cuales deberán ser incluidos en el informe.

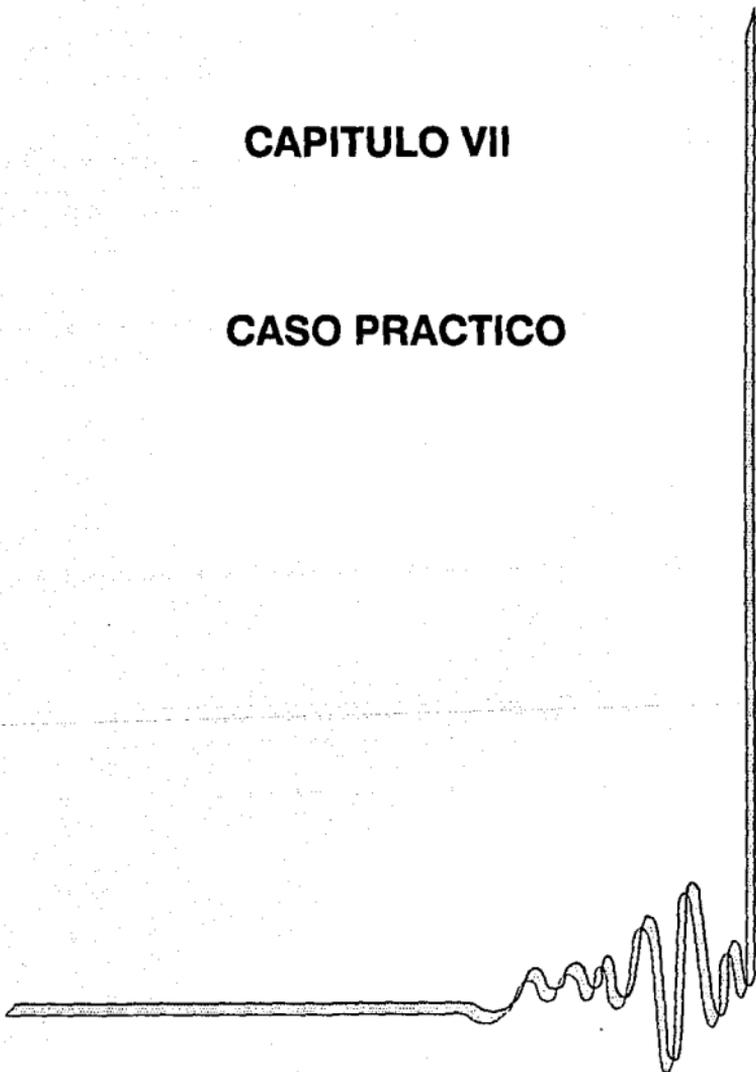
6.4. SEGUIMIENTO DE LAS OBSERVACIONES DEL INFORME

Cuando por el resultado de las observaciones y recomendaciones contenidas en el informe de auditoría se deban tomar medidas correctivas, el auditor se cerciorará de que éstas se han puestas en vigor oportunamente, y que permitan alcanzar los resultados deseados.

Cuando no se hayan tomado las medidas sugeridas en asuntos que, a juicio del auditor, sean importantes para el logro de los objetivos o de la eficiencia de las áreas auditadas, hará constar este hecho en los informes que presente posteriormente ante los niveles competentes.

CAPITULO VII

CASO PRACTICO



CAPITULO VII

CASO PRACTICO

En esta parte se inicia la auditoría describiendo su alcance, la metodología y etapa por etapa el resultado de la misma .

ALCANCE DE LA AUDITORIA

La metodología presentada estará enfocada a los siguientes aspectos :

Seguridad
Eficiencia y desempeño de la red
Administración de la red

Seguridad

En la seguridad se evaluará al nivel físico y lógico donde se cubrirá : aplicaciones, hardware, software, operación y administración. Además, se revisarán los planes de contingencia.

Eficiencia y Desempeño

Para la eficiencia se analizará la optimización de costos y para el desempeño la calidad de la red (tiempo de respuesta, disponibilidad, versatilidad, etc.).

Administración de la Red

Se verán las políticas, procedimientos, parámetros y controles establecidos para la administración adecuada de la red.

Para cubrir estos aspectos en una forma ordenada se cuenta con cinco pasos.

DEFINIR BASE INSTALADA

Teniendo como finalidad determinar los componentes físicos, lógicos y las aplicaciones principales de la red.

Nuestro primer objetivo es conocer las aplicaciones bancarias que hacen uso de la red de telecomunicaciones y los porcentajes en que la utilizan cada una de ellas.

Para lo cual es necesario que el auditor tenga la información necesaria para poder responder a las siguientes preguntas :

- ¿ Cuáles son las aplicaciones que utilizan la red ?
- ¿ Con qué frecuencia la utilizan estas aplicaciones ?
- ¿ Cuáles son los niveles de tráfico en cada aplicación ?
- ¿ Definir los servicios que ofrece la red ?
- ¿ Cuáles de estos servicios se utilizan ?
- ¿Cuál es el crecimiento estimado de tráfico por cada una de las aplicaciones en corto plazo ?
- ¿Cuál es la razón por la que no se utilizan algunos servicios ?

Por lo que empezaremos definiendo las actividades bancarias.

En los antecedentes de esta tesis se definió lo que es una Sociedad Nacional de Crédito (S.N.C.) y sus actividades bancarias, ahora daremos un panorama general de los servicios que ofrece la banca, siendo importante conocerlos para tener una idea de las necesidades de cómputo y comunicaciones.

SERVICIOS QUE OFRECEN LAS SOCIEDADES NACIONALES DE CREDITO

- 1) Servicios que promueven la captación de recursos.
 - Cuenta de ahorros
 - Cuenta de cheques
 - Cheque certificado
 - Cheque de caja
 - Cheque de ventanilla
 - Pago de cheques oficiales

2) **Créditos bancarios.**

- Préstamos personales
- Préstamos prendarios
- Préstamos refaccionarios
- Préstamos quirografarios
- Préstamos hipotecarios
- Préstamo de habilitación o avío
- Tarjetas de crédito
- Descuentos
- Préstamos para la adquisición de bienes de consumo duradero
- Créditos comerciales

3) **Servicios Nacionales e Internacionales.**

- Remesas en camino sobre el país y el extranjero
- Cobranzas del interior y del extranjero
- Ordenes de pago
- Compra venta de giros bancarios internacionales y nacionales
- Compra venta de moneda extranjera y oro
- Venta de cheques de viajero

4) **Servicios relacionados con valores.**

- Compra venta de valores
- Futuros

5) **Servicios relacionados con fiduciario.**

- Avalúos
- Compra venta de inmuebles
- Fideicomiso
- Mandatos

6) **Otros servicios.**

- Pago de servicios con cargo a la cuenta de cheques
- Alquiler de cajas de seguridad

En el Anexo I se encuentran las definiciones a los servicios mencionados.

Ahora mencionaremos los servicios que hacen uso de la red, y el número de transacciones por día, además, de la frecuencia de utilización.

SERVICIO	NUMERO DE	FRECUENCIA TRANSAC.	OBSERVACIONES	
Aplicaciones fuera de línea	2,065	día	Promedio	
Sucursales en línea	Cheques	18,620	día	Promedio
	Inversiones	7,155	día	Promedio
	Divisas	1,789	día	Promedio
	Ahorro	4,223	día	Promedio
Cajeros en línea	Locales	1,300	día	Promedio
	Foráneos (60)	1,800	día	Promedio
Remesas	4,200	día	Promedio	
Tarjetas de crédito y débito (POS)	10,400	día	Promedio	
Ordenes de pago	450	día	Promedio	
Recursos humanos	Local	10	mes	Promedio
	Foráneos	15	mes	Promedio
Sistemas administrativos	1.5	mes	Promedio	
Banco en su empresa	Local	30	día	Promedio
	Foráneo		día	Promedio
Transacciones de mesa de dinero	5,000	día	Promedio	

Los servicios que ofrece la red de comunicaciones son los de :

- VOZ
- DATOS

Para voz la utilización es mínima aproximadamente un 10% ya que este servicio se esta dando únicamente por medio de enlaces vía satélite; sin embargo, el uso que se le da para datos es del 90 %.

Las Características principales del Banco son :

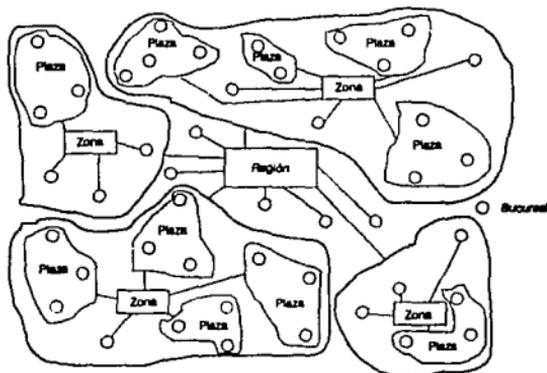
Se tiene cobertura a nivel nacional, con sucursales en toda la República.

Se encuentra dividido en 6 regiones las cuales son autónomas en su administración.

A su vez cada región se encuentra dividida en zonas, las cuales reportan directamente.

Las plazas son un conjunto de sucursales las cuales dependen de una zona por su situación geográfica

Es importante mencionar que una sucursal puede reportar tanto a una región, zona, o plaza sin olvidar que en un determinado momento una sucursal puede ser una plaza.



EJEMPLO DE DISTRIBUCION DE UNA REGION

Las regiones son puntos estratégicos para el banco, donde por su actividad bancaria (económica) se justificó tener un centro de cómputo, donde se pudiera controlar exclusivamente un área geográfica de la República.

Al paso del tiempo la actividad bancaria en las regiones se incremento notablemente lo que dio como origen la creación de zonas que son un subconjunto de las regiones, y de la misma forma fue que se crearon las plazas que son un subconjunto de las zonas.

Siendo una estrategia y necesidad bancaria se decide crear una infraestructura para poder competir con la banca nacional y extranjera teniendo como objetivo la calidad y eficiencia del servicio.

Por lo anterior, el banco toma la decisión de crear una red de telecomunicaciones que brinde principalmente dos servicios :

- 1) Transferencia de archivos (Concentración y dispersión de información).
- 2) Diálogo de transacciones.

Ya que mencionamos las principales aplicaciones de la red tendremos un nuevo objetivo que es recolectar la información necesaria para realizar el estudio de la red de telecomunicaciones a auditar, para esto es necesario que el auditor cuente con la información necesaria para contestar las siguientes preguntas :

¿ Se cuenta con un inventario de la red ?

¿ Quién lleva el inventario ?

¿ Cómo lo administra ?

¿ Qué información tiene ?

¿ Con qué frecuencia se actualiza el inventario ?

Solicitar una copia del inventario.

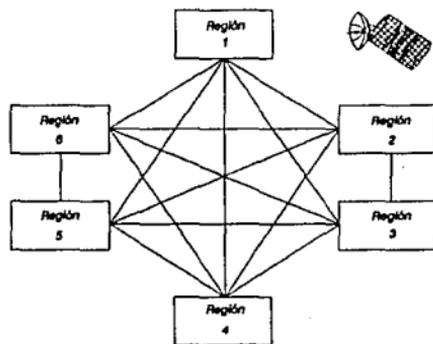
Solicitar diagrama de la red a auditar.

La información solicitada se dará de dos formas, la primera dando un panorama general de la red y la segunda especificando cada región.

BASE INSTALADA

Para atender los diferentes servicios descritos, el Banco cuenta con una red de telecomunicaciones con 6 nodos principales (Sistemas Unisys 2200), distribuidos en las diferentes regiones; a su vez, en cada región se encuentran un número de maquinas IBM S/38 (Sistema 38) conectadas a las Unisys dependiendo de las necesidades de la región y además se tiene un equipo IBM S/38 en la región central dedicado al monitoreo de todos los puntos de la red, para cuidar el buen funcionamiento de la misma.

Los equipos Unisys se encuentran conectados a través de una red X.25 vía satélite. En cada región se tiene una arquitectura SNA (System Netware Architecture) para conectar los equipos IBM con el sistema Unisys por diferentes medios utilizando el protocolo SDLC (Synchronous Data Link Control)



RED RADIADA

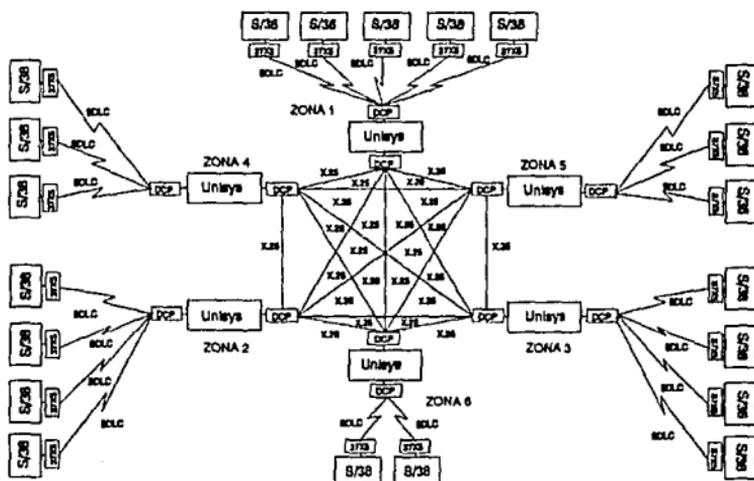
En las regiones se tienen conectados diferentes tipos de cajeros automáticos.

La relación de equipos IBM S/38 conectados en cada región es la siguiente :

- Región 1 : 5 Sistemas IBM 38
- Región 2 : 4 Sistemas IBM 38
- Región 3 : 4 Sistemas IBM 38
- Región 4 : 3 Sistemas IBM 38

- Región 5 : 3 Sistemas IBM 38
- Región 6 : 2 Sistemas IBM 38

El siguiente diagrama nos da una idea general de la manera en que están conectados los equipos principales así como los diferentes protocolos utilizados. En la configuración se utilizan dos tipos de FEPs (Front End-Processors), el 37X5 de IBM y el DCP (Distributed Communications Processors) de Unisys.

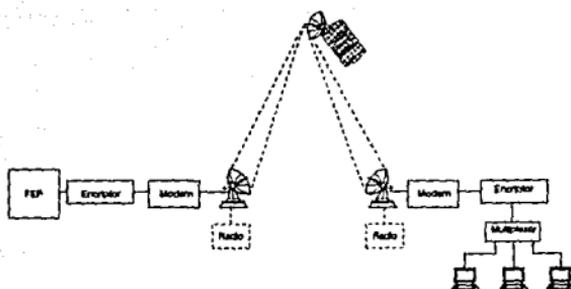


PROTOSCOLOS Y EQUIPOS PRINCIPALES DE LA RED

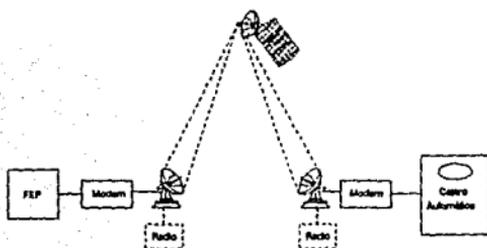
Las diferentes características de los S/38 de IBM, Unisys 2200 y los FEPs se incluyen en el Anexo II.

A lo largo de la red se cuenta con 5 diferentes tipos de enlace para conectar las terminales o los cajeros automáticos. El tipo de FEP utilizado para los enlaces depende del tipo de máquina a la se conecte (IBM/Unisys).

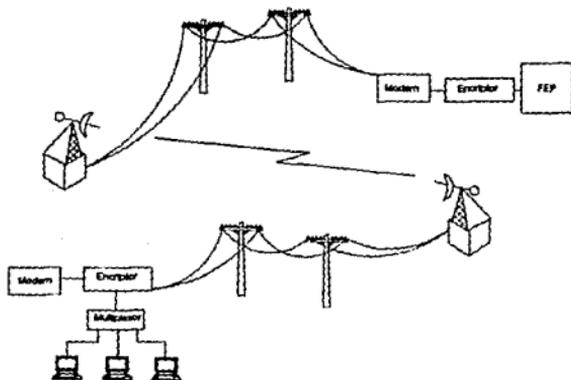
El primer enlace es por vía satélite. Este enlace es usado para comunicar los diferentes cajeros remotos y algunas sucursales, con una velocidad de transmisión de 64 Kbps.



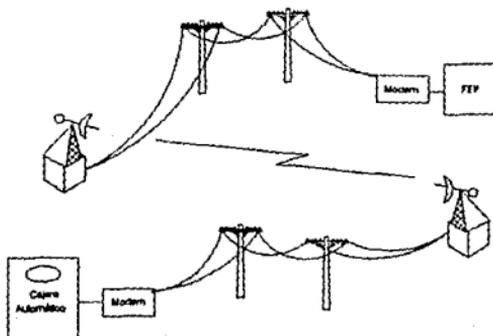
ENLACE POR SATELITE



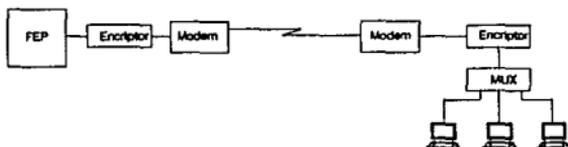
El segundo enlace es vía microondas, la información se transmite a través de ondas de radio de muy corta longitud, por este medio se comunican algunas sucursales y cajeros automáticos.



ENLACE POR MICROONDAS



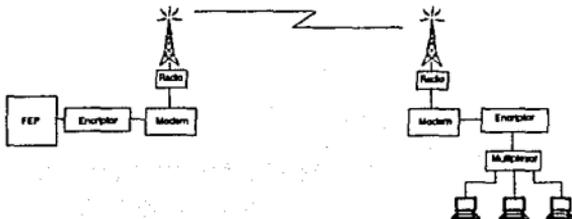
El tercer enlace es por línea privada, por este medio se comunican algunas sucursales, terminales y cajeros automáticos a una velocidad de 9.6 Kbps.



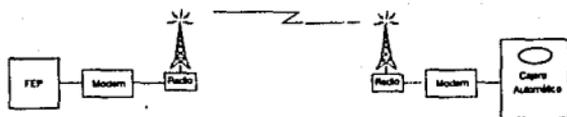
LINEAS PRIVADAS



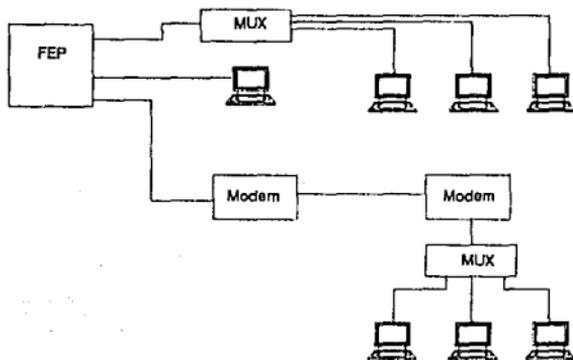
El cuarto enlace es vía radio, por este medio se comunican algunas sucursales y cajeros automáticos.



ENLACE POR RADIO



El quinto enlace es para las terminales locales, es decir, aquellas que se encuentran en el mismo edificio.

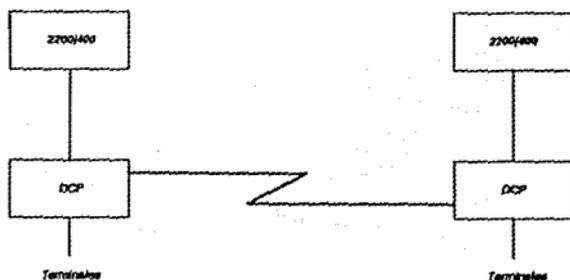


LINEAS LOCALES

Los modems utilizados son de diferentes marcas y con características diferentes, por mencionar alguno, el modem satélital SM290 Fairchild.

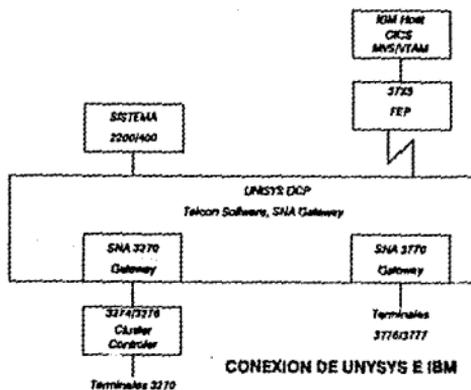
Para conectar un sistema Unisys 2200 a otro sistema Unisys, se tiene un procesador de comunicaciones con software Telcon, esta combinación tiene un gran alcance y versatilidad en las redes.

Los sistemas Unisys están conectados entre sí vía DCPs.



CONEXION DE UNISYS A UNISYS

Y las máquinas IBM S/38 están conectados vía Gateway con los sistemas Unisys.



CONEXION DE UNISYS E IBM

Ya que se tiene un panorama general de la red, estudiaremos cada una de las diferentes regiones.

A continuación mostraremos los inventarios del equipo de comunicaciones de las regiones en forma de tabla.

Es importante hacer notar que algunas columnas de nuestras tablas están en blanco por considerarse información confidencial del Banco.

RELACION DE EQUIPO DE LA REGION I

MARCA	DESCRIPCION	MODELO	INSTALADOS	POR INSTALAR	RESPALDO	TOTAL	PROPIO	RENTADO
UNISYS	EQUIPO MACRO	2200	1	-	-	1	1	-
IBM	EQUIPO MINI	S/38	5	-	-	5	5	-
	CAJERO AUTOMATICO		18	2	-	20	20	-
	TERMINAL ON-LINE	XX	83	-	5	88	88	-
	TERMINAL ON-LINE	YY	175	22	15	212	212	-
	IMPRESORAS		208	22	5	235	235	-
	MODEMS		100	-	12	112	112	-
	MODEMS (SATELITE)		6	-	1	7	7	-
	CONTROLADOR DE TERMINALES		12	-	4	16	16	-
	EQUIPO DE MONITOREO Y CONTROL		5	-	-	5	5	-
	TERMINALES DE MONITOREO		10	-	1	11	11	-
	ENCRIPTORES		100	-	5	105	105	-
	RADIOS		20	-	4	24	24	-
	MULTIPLEXOR		3	-	1	4	4	-
IBM	FEP	37XS	5	-	1	6	6	-
UNISYS	DCP	40	2	-	1	3	3	-

RELACION DE EQUIPO DE LA REGION 2

MARCA	DESCRIPCION	MODELO	INSTALADOS	POR INSTALAR	RESPALDO	TOTAL	PROPIO	RENTADO
UNISYS	EQUIPO MACRO	2200	1	-	-	1	1	-
IBM	EQUIPO MINI	S/R	4	-	-	4	4	-
	CAJERO AUTOMATICO		10	5	-	15	15	-
	TERMINAL ON-LINE	XX	23	-	7	30	30	-
	TERMINAL ON-LINE	YY	40	-	5	45	45	-
	IMPRESORAS		38	-	6	44	44	-
	MODEMS		50	-	5	55	55	-
	MODEMS (SATELITE)		6	-	1	7	7	-
	CONTROLADOR DE TERMINALES		7	-	3	10	10	-
	EQUIPO DE MONITOREO Y CONTROL		3	-	-	3	3	-
	TERMINALES DE MONITOREO		6	-	1	7	7	-
	ENCRIFTORES		50	-	3	53	53	-
	RADIOS		16	-	2	18	18	-
	MULTIPLEXOR		2	-	1	3	3	-
IBM	FEP	37X5	4	-	1	4	4	-
UNISYS	DCP	40	2	-	1	3	3	-

RELACION DE EQUIPO DE LA REGION 3

MARCA	DESCRIPCION	MODELO	INSTALADOS	POR INSTALAR	RESPALDO	TOTAL	PROPIO	RENTADO
UNISYS	EQUIPO MACRO	2200	1	-	-	1	1	-
IBM	EQUIPO MINI	S/38	4	1	-	4	4	-
	CAJERO AUTOMATICO		15	-	-	15	15	-
	TERMINAL ON-LINE	XX	15	-	2	17	17	-
	TERMINAL ON-LINE	YY	40	11	7	58	58	-
	IMPRESORAS		30	2	3	35	35	-
	MODEMS		50	-	6	56	53	-
	MODEMS (SATELITE)		6	-	1	7	7	-
	CONTROLADOR DE TERMINALES		7	-	3	10	10	-
	EQUIPO DE MONITOREO Y CONTROL		3	-	-	3	3	-
	TERMINALES DE MONITOREO		6	-	1	7	7	-
	ENCRIPTORES		50	-	3	53	53	-
	RADIOS		16	-	2	18	18	-
	MULTIPLEXOR		2	-	1	3	3	-
IBM	FEP	37X5	4	-	1	4	4	-
UNISYS	DCP	40	2	-	1	3	3	-

RELACION DE EQUIPO DE LA REGION 4

MARCA	DESCRIPCION	MODELO	INSTALADOS	POR INSTALAR	RESPALDO	TOTAL	PROPIO	RENTADO
UNISYS	EQUIPO MACRO	2200	1	-	-	1	1	-
IBM	EQUIPO MINI	S/38	3	-	-	3	3	-
	CAJERO AUTOMATICO		8	3	-	11	11	-
	TERMINAL ON-LINE	XX	10	-	3	13	13	-
	TERMINAL ON-LINE	YY	35	5	4	44	44	-
	IMPRESORAS		26	-	3	29	29	-
	MODEMS		38	-	4	42	42	-
	MODEMS (SATELITE)		6	-	1	7	7	-
	CONTROLADOR DE TERMINALES		5	-	2	7	7	-
	EQUIPO DE MONITOREO Y CONTROL		3	-	-	3	3	-
	TERMINALES DE MONITOREO		6	-	1	7	7	-
	ENCRIPTORES		38	-	2	40	40	-
	RADIOS		10	-	2	12	12	-
	MULTIPLEXOR		1	-	1	2	2	-
IBM	FEP	37X5	3	-	1	4	4	-
UNISYS	DCP	40	2	-	1	3	3	-

RELACION DE EQUIPO DE LA REGION 5

MARCA	DESCRIPCION	MODELO	INSTALADOS	POR INSTALAR	RESPALDO	TOTAL	PROPIO	RENTADO
UNISYS	EQUIPO MACRO	2200	1	-	-	1	1	-
IBM	EQUIPO MINI	S/8	3	-	-	3	3	-
	CAJERO AUTOMATICO		18	1	-	19	19	-
	TERMINAL ON-LINE	XX	16	-	3	19	19	-
	TERMINAL ON-LINE	YY	35	-	3	38	38	-
	IMPRESORAS		32	2	3	37	37	-
	MODEMS		38	-	6	44	44	-
	MODEMS (SATELITE)		6	-	1	7	7	-
	CONTROLADOR DE TERMINALES		4	-	2	6	6	-
	EQUIPO DE MONITOREO Y CONTROL		3	-	-	3	3	-
	TERMINALES DE MONITOREO		6	-	1	7	7	-
	ENCRIPTORES		38	-	3	41	41	-
	RADIOS		12	-	2	14	14	-
	MULTIPLEXOR		1	-	1	2	2	-
IBM	FEP	37X5	3	-	1	3	3	-
UNISYS	DCP	40	2	-	1	3	3	-

RELACION DE EQUIPO DE LA REGION 6

MARCA	DESCRIPCION	MODELO	INSTALADOS	POR INSTALAR	RESPALDO	TOTAL	PROPIO	RENTADO
UNISYS	EQUIPO MACRO	2200	1	-	-	1	1	-
IBM	EQUIPO MINI	S/38	2	-	-	2	2	-
	CAJERO AUTOMATICO		5	3	-	8	8	-
	TERMINAL ON-LINE	XX	6	-	1	7	7	-
	TERMINAL ON-LINE	YY	25	2	2	29	29	-
	IMPRESORAS		19	-	2	21	21	-
	MODEMS		24	-	3	27	27	-
	MODEMS (SATELITE)		6	-	1	7	7	-
	CONTROLADOR DE TERMINALES		3	-	1	4	4	-
	EQUIPO DE MONITOREO Y CONTROL		1	-	-	1	1	-
	TERMINALES DE MONITOREO		2	-	1	3	3	-
	ENCRIPTORES		24	-	1	25	25	-
	RADIOS		6	-	1	7	7	-
	MULTIPLEXOR		1	-	1	2	2	-
IBM	FEP	37X5	2	-	1	3	3	-
UNISYS	DCP	40	2	-	1	3	3	-

SEGURIDAD DE LA RED

SEGURIDAD ADMINISTRATIVA DE LA RED.

La parte administrativa del departamento de telecomunicaciones es la encargada de la seguridad de la red, para verificar la seguridad se tienen diversos medios entre los cuales existe un software que reporta las claves bloqueadas por intentos de conexión y todos los puntos conectados en un momento determinado.

Existen diferentes tipos de reportes que ayudan a administrar la red, los cuales se pueden demandar en cualquier momento o al dar de baja el sistema.

Para dar seguimiento a estos reportes se alimenta una base de datos que compara las cifras contra un promedio diario normal, si este promedio se excede se entrega el reporte al jefe del departamento para dar investigación a estas anomalías.

Este procedimiento se encuentra estandarizado a nivel nacional ya que el software reporta a diferentes niveles como pueden ser los administrativos de las diferentes regiones, zonas o plazas.

Cuando se realiza un cambio al software se busca que este no afecte los diferentes procesos que lo utilizan y por pequeño que sea el cambio el área administrativa se encarga de emitir las normas de adecuación a los cambios.

Este departamento se encuentra abierto para que cualquier usuario de la red pueda enviar o hacer cualquier observación sobre la operación de la Red.

Software para la Seguridad de la Red.

Dentro de la Institución no se cuenta con un software específico para la seguridad, ya que el sistema operativo nos brinda la facilidad para asignar diferentes tipos de privilegios a usuarios o grupos de usuarios además diferentes derechos por archivos para usuarios o grupos.

El control de las claves de acceso es administrado por un departamento encargado de asignarlas, y de incluir a los usuarios dentro de un grupo de usuarios con ciertos privilegios. Cuando una clave de acceso es requerida por alguna persona o departamento, se envía un comunicado y el departamento encargado, asigna las claves de acceso y un password temporal, notifica el alta de la clave y password al propietario de la clave, y se recomienda que cambie su password a la brevedad posible, el propietario de la clave tiene la facultad de cambiar el password en cualquier momento. Por otra parte el sistema operativo tiene la facultad de exigir el cambio de password en un tiempo definido por el operador del sistema por usuario, el sistema al momento de recibir una alta de clave pide un password.

El sistema cuenta con una herramienta para bloquear una clave si esta tiene 3 intentos fallidos al digitar el password y solo una clave privilegiada con nivel de administrador de la red es la única facultada para desbloquear estas claves. Cuando una clave es bloqueada se incluye en uno de los reportes del sistema, para dejar un antecedente, además, se imprime en la consola del operador.

Todas las terminales conectadas a la red tienen una identificación única por hardware y este número esta controlado por los sistemas concentradores para controlar las diferentes rutas de acceso, si una terminal intenta ser conectada sin estar registrada en esa ruta no se le permite el acceso, todos estos intentos son registrados en un reporte.

Existe una herramienta para conocer el número de usuarios activos en un momento preciso, con esta herramienta se puede saber el dueño de la clave, la ubicación de la terminal y se puede enviar mensajes a este usuario.

Algunos de los reportes que emite el sistema son utilizados por el departamento de auditoría de sistemas para evaluar la operación de la red.

Hardware para la Seguridad de la Red.

En la Institución el principal medio de seguridad por hardware de la red lo representan los FEPs y los encriptores de información.

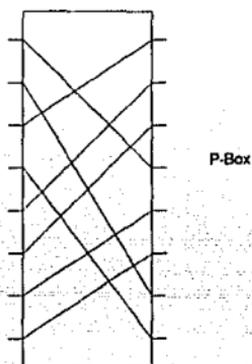
Los FEPs se consideran como parte de la seguridad, puesto que estos tienen un sistema para ser programados para aceptar únicamente las conexiones que se especifican, estas conexiones se identifican con un número que tiene cada equipo terminal.

Por otro lado se cuenta con encriptores, estos se utilizan en todas las transmisiones remotas (únicamente microondas). El método de encriptación utilizado es el DES (Data Encryption Standard).

Consideramos que es importante explicar el método DES, por ser un estándar seguro y económico para proteger la información.

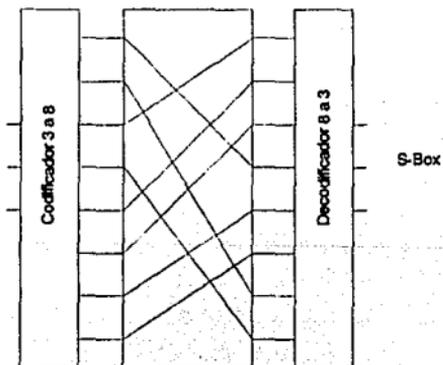
Para poder explicar el DES es necesario conocer las bases tradicionales de encriptamiento : la transposición y la sustitución.

La transposición y la sustitución pueden implementarse con circuitos simples. El circuito para la transposición es conocido como P-Box.



En el circuito particular del dibujo si 8 bits son designados de arriba hacia abajo como 01234567, la salida del P-Box sería 36071245.

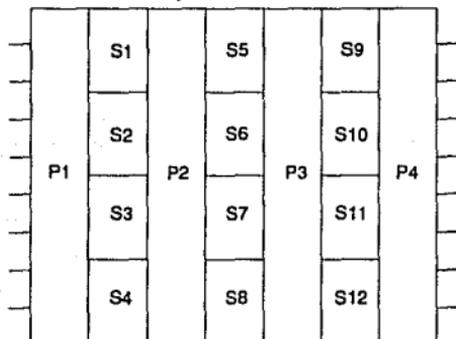
El circuito para la sustitución es conocido como S-Box.



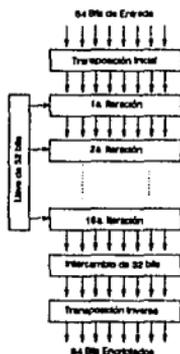
En este ejemplo tenemos que 3 bits entran y 3 salen encriptados, los 3 bits seleccionan una de las 8 líneas del primer estado y la ponen en 1; las demás líneas son 0. El segundo estado es un P-Box y el tercer estado decodifica la salida en binario nuevamente. Por ejemplo si los siguientes 8 números 012345678 son introducidos uno detrás de otro, la secuencia sería 24506713.

El poder de estos circuitos se ve cuando son conectados en cascada.

S-Box y P-Box en Cascada



Para describir el algoritmo de DES es necesario representarlo en un diagrama.



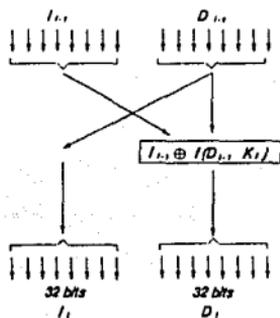
ESQUEMA GENERAL DEL DES

La información es encriptada en bloques de 64 bits. El algoritmo utiliza un parámetro de 56 bits (llave) y tiene 19 estados distintos. El primer estado es una transposición de los 64 bits con un P-Box. El último estado es exactamente la inversa de la transposición inicial.

El penúltimo cambia los 32 bits menos significativos con los 32 bits más significativos. Los otros 16 estados son funcionalmente iguales pero son parametrizados por diferentes funciones llave.

El algoritmo para descryptar utiliza las mismas llaves y los pasos son los mismos pero se ejecutan en orden inverso.

La operación de uno de estos estados intermedios se ilustra a continuación.



DETALLE DE UNA ITERACION

Este estado divide los 64 bits en 2 grupos de 32 bits. La salida izquierda es simplemente una copia de la entrada derecha. La salida derecha es el resultado de una XOR (or exclusiva) de la entrada izquierda y una función de la entrada derecha y la llave para este estado, K_i .

La función consiste de 4 pasos, que se ejecutan en secuencia. Primero un número de 48 bits, E, es generado por expansión del grupo D_{j-1} de 32 bits de acuerdo a una transposición y una regla de duplicidad. El segundo, E y K_j se operan con XOR. El resultado es particionado en 8 grupos de 6 bits. Cada uno es procesado en un diferente S-Box. Los S-Boxes producen 4, en lugar de 6 bits de salida. Una de las 64 posibles entradas al S-Box es mapeada en una salida de 4 bits. El resultado es una lista de 8 grupos de 4 bits. Finalmente, estos 32 bits son pasados por un P-Box.

La versatilidad de este sistema estriba en poder utilizar diferentes llaves y utilizar diferentes tipos de funciones.

Continuando con la revisión del hardware detectamos que para la verificación de claves de acceso no existe un hardware ya que esta función es del software del sistema (sistema operativo).

Al revisar los encriptores de la región central pudimos observar que todas las transmisiones pasaban por un encriptador pero algunos de los encriptores estaban desactivados por necesitar mantenimiento y otros en "bypass", es decir, solo se usa de puente por que la información que recibe es exactamente la que entrega, lo que implica que en el otro extremo de la línea se encuentra también desactivado el encriptador, lo que nos indica la falta de encriptores de respaldo.

Los encriptores reciben un mantenimiento preventivo cada 6 meses por parte de una empresa externa.

Para verificar el buen funcionamiento de los encriptores al conectarse estos mandan una secuencia de prueba para verificar el buen funcionamiento de la línea, del encriptador del otro extremo y del mismo encriptador.

El departamento de Telecomunicaciones es el encargado de llevar el control de los encriptores, es decir, se encarga de la conexión, contratar el mantenimiento y lleva un inventario por medio de una base de datos, donde controla la ubicación física del encriptador, a los equipos que se conecta y la persona encargada del mismo. Sería bueno incluir en esta base de datos el control de mantenimiento del equipo ya que este se lleva en forma manual por otro sistema.

Planes de Contingencia

El edificio que aloja el centro de comunicaciones es una construcción moderna para diferentes propósitos, como alojar personal de oficinas, equipo de cómputo y equipo de comunicaciones, etc.

El centro de cómputo y el lugar donde se encuentra el equipo de telecomunicaciones esta protegido con equipo contra incendios, además de ser un lugar resistente.

El equipo esta asegurado contra siniestros, en una compañía nacional de seguros.

Todos los equipos en general se encuentran aterrizados en forma correcta y se cuenta con tierra física para las antenas y torres del edificio.

Todos los contactos de la sala de comunicaciones y los equipos de cómputo en general son polarizados y se encuentran conectados a un sistema "no-brake", que con carga máxima da un tiempo de 20 minutos aproximadamente, en lo que entra la planta de emergencia a base de combustible.

Al evaluar los enlaces en los diferentes puntos de la red, se observaron diferentes medios de comunicaciones como son radio, líneas privadas, microondas, etc. En los puntos más importantes se cuenta con un sistema alterno para utilizarlo cuando no se pueda establecer por medio del primario. Cuando se pierde comunicación con un punto que no tiene enlace alterno se trabaja fuera de línea y los documentos se envían a la cabecera de la región.

Nunca se ha realizado una evaluación de los riesgos y amenazas probables a la red, lo único que se prevee es la falla de algún equipo o de las líneas de comunicación.

Cuando uno de los sistemas se interrumpe en forma no deseada, el sistema cuenta con una herramienta de recuperación, fácil de entender ya que se trata de un sistema transaccional, en donde se lleva un contador de las transacciones procesadas, cuando el sistema se interrumpe, se tiene los números de las últimas transacciones realizadas, cuando el sistema se recupera envía a los puntos que estaban conectados al momento de la interrupción el número de la última transacción terminada, y el protocolo de comunicaciones se encarga de retransmitir todas las transacciones pendientes.

Existen diferentes tipos de planes de contingencia dependiendo del problema que se tenga, por ejemplo cuando un medio de comunicación falla, se conecta el sistema alterno. Cuando un equipo de comunicaciones llega a fallar se conectan las líneas más importantes a otro DCP y se configura para que las acepte en lo que se conecta el DCP que se tiene de respaldo. Cuando se detecta una cierta cantidad de humo en la sala de máquinas se conecta en forma automática el sistema de emergencia a base de gas y se da un "down" de emergencia en forma automática para después interrumpir la corriente eléctrica, este procedimiento se puede interrumpir en forma automática. La temperatura, humedad y el humo son censados en forma constante por detectores colocados en lugares estratégicos. En general para cualquier tipo de contingencia se actúa de manera similar.

El sistema toma en cuenta el manejo de datos críticos, siempre que se tienen este tipo de datos se les da prioridad de transmisión y procesamiento, es decir, se tiene catalogadas las transacciones con diferentes prioridades.

Los sistemas de seguridad con que se cuenta son probados en forma regular aproximadamente cada 2 meses y cuando se detecta algún problema se corrige de inmediato dada la importancia de los mismos.

Los procedimientos de emergencia se diseñaron de acuerdo a las necesidades de la Institución y son revisados en forma regular.

Estos planes fueron desarrollados por diferentes departamentos, el diseño del edificio que aloja las instalaciones de comunicaciones fue realizado de acuerdo a las especificaciones de la compañía, los planes de contingencia en caso de desastres fueron implementados por una comisión organizada de profesionistas y especialistas en desastres. Los planes de contingencia para combatir las fallas del equipo de comunicaciones fueron diseñadas en su mayoría por el departamento de telecomunicaciones que son las personas que tienen experiencia al respecto.

Estos planes se dan a conocer a todos los empleados de cada área por medio de boletines que tienen que de enterados.

También se dan cursos para conocer estos planes de contingencia y principalmente que hacer en caso de siniestros, existen comisiones encargadas de la seguridad de cada departamento a nivel Institucional.

Se hacen simulacros de algunos de estos planes de contingencia y otros se han puesto en práctica, como por ejemplo, problemas con la comunicación, fallas del equipo de comunicaciones y caídas del sistema principalmente.

En cada departamento en forma general se encuentran organizadas brigadas para actuar en caso de contingencia, el departamento de telecomunicaciones tiene gente responsable con diferentes tareas, esto es controlado por el jefe del departamento y lo reporta en forma trimestral a sus superiores, así como el desempeño de cada persona.

Cuando se tiene que decidir sobre algunos procesos o enlaces, el responsable de la operación que se encuentre lo decidirá, de acuerdo a lo establecido en el plan de contingencia.

Estas prioridades están determinadas por el nivel de las transacciones, es decir, cuando se tiene que decidir entre atender dos transacciones se atiende a la de menor número (mayor prioridad) y en cuanto a actuar en un momento dado dependerá de la experiencia del personal para tomar decisiones de que atender primero.

SEGURIDAD FISICA

Controles de Fuego.

La edificación que aloja el centro de cómputo y las instalaciones de comunicaciones fue construida en general con material poco flamable.

Las instalaciones mencionadas se encuentran en una especie de bóveda con las seguridades que la misma exige.

Las impresoras se encuentran alejadas del sistema de comunicaciones y de cómputo. Se tienen diferentes centros de impresión ubicados de acuerdo a las necesidades de los diferentes usuarios. Por lo cual no se tiene riesgo de tener demasiado papel en las instalaciones, el único papel que se tiene es el utilizado por las consolas del sistema, pero se cuida que únicamente se tenga el necesario.

En general en el centro de cómputo y área de telecomunicaciones esta prohibido fumar. A lo largo de las instalaciones se cuenta con extinguidores de tipo ABC. La gerencia de seguridad da cursos obligatorios en donde se enseña el uso de los diferentes tipos de extinguidores.

El personal de operación tomo un curso especial de seguridad en una de las compañías distribuidoras del equipo.

El centro de cómputo y las instalaciones de comunicaciones cuentan con detectores de humo que activan en forma automática, las alarmas y los extintores automáticos de gas, con este equipo hay que tener mucho cuidado ya que cualquier cantidad de humo (dos personas fumando) los activan y es un sistema muy caro. La energía eléctrica se desactiva después de darse un "down" de emergencia en forma automática cuando una alarma esta activada.

El personal de seguridad de acceso a las instalaciones tiene el control de la energía eléctrica, y en la oficina de telecomunicaciones se tiene un control adicional que desactiva la calefacción, ventilación y aire acondicionado, pero este se desactiva en forma automática.

No se tiene una lista de comprobación para apagar el equipo.

Nunca se han hecho simulacros de incendio en el área.

No existen cajillas de alarma de incendios, pero se puede activar en forma sencilla el sistema de alarma en la entrada del centro.

Al activarse la alarma esta suena en el centro de cómputo, instalaciones de telecomunicaciones y departamento de seguridad únicamente.

En caso de falla eléctrica, entra en funcionamiento el equipo "no-brake" y arranca la planta de emergencia, algunas de las luces del centro están conectadas a este sistema y se considera que son suficientes para actuar en esos momentos.

Controles de Agua.

El equipo se encuentra ligeramente arriba del nivel del suelo por que se utiliza subsuelo para las conexiones, pero el centro esta protegido contra inundaciones.

Sobre el centro de cómputo y telecomunicaciones si pasan tuberías que surten otros departamentos, pero se tiene protegidos los departamentos por una bóveda.

Las puertas del centro son selladas, por lo tanto están protegidas contra el agua.

Sin embargo, esto es a nivel central, en algunas localidades como plazas estas medidas no son muy buenas.

Controles de Electricidad.

En cuanto al suministro eléctrico por parte de las dependencias externas no es muy confiable dado que se tienen muchos problemas en los tiempos de lluvia, pero en general en todas las cabeceras de área se cuenta con plantas de emergencia y sistemas "no-brake".

El nivel de la energía suministrada esta siendo registrado en forma constante y además se cuenta con equipo regulador de corriente.

Los cables del centro de cómputo no siguen ningún estandar de colores, pero son los adecuados de acuerdo a la cantidad de energía que conducen.

Controles de Acceso.

Las instalaciones del centro de cómputo y telecomunicaciones, son semejantes a una fortaleza, ya que todas las paredes, techo y suelo son seguros, la entrada a las instalaciones es controlada por medio de credenciales que se insertan en torniquetes, además hay personal de seguridad en la entrada.

Los torniquetes de acceso, permiten la entrada únicamente a las personas autorizadas, cuando el torniquete no permite la entrada a una persona, el personal de seguridad exige un memorándum donde se especifica el nombre de la persona que se autoriza entrar a las instalaciones y el motivo, este memorándum debe estar autorizado por el gerente de sistemas.

Las instalaciones están vigiladas las 24 hrs.

El centro de cómputo tiene únicamente una entrada/salida por cuestión de seguridad y tiene una salida de emergencia.

Controles de Aseo y Mantenimiento

Diariamente personal de limpieza hace el aseo en presencia de una persona de seguridad, el equipo en general se limpia cuando se le da el mantenimiento preventivo, el interior de los pisos falsos no se limpia con regularidad. El personal de limpieza entra con bolsas de polietileno grandes y vacía los botes de basura que se encuentran en el centro, esto posiblemente aumente la cantidad de polvo que se produce en el centro. Esta prohibido en forma estricta el introducir alimentos al centro así como fumar.

Controles de Asuntos Generales

El centro de cómputo y comunicaciones se encuentra dentro de un edificio que esta vigilado las 24 hrs.

No se ha capacitado para manejar amenazas de bombas. No existe ningún programa de enlace con alguna agencia de orden público.

SEGURIDAD DE TRANSMISION

PROTOCOLOS DE TRANSMISION DE LA RED

La seguridad de la transmisión esta principalmente controlada por los protocolos y los encriptores utilizados.

Synchronous Data Link Control (SDLC)

SDLC es un protocolo orientado a bits, la información es transmitida en unidades llamadas "frames" (Estructuras). Con SDLC el texto es transmitido en EBCDIC. Un frame siempre inicia y termina con una bandera. Esta bandera es 01111110 = 7EH. La siguiente figura nos muestra la estructura de un frame.

Bandera	Dirección	Campo de Control	(Texto)	FCS	Bandera
Bits: 8	8	8	Múltiplos de 8	16	8

Existen varias maneras de conformar una bandera para terminar un frame e iniciar el próximo frame.

Frame X | Frame X+1

- (a) 01111110|01111110...
- (b) 011111101111110....
- (c) 01111110
- (d) ..01111110|01111110 01111110|0111111..

- (a) Dos banderas separadas totalmente
- (b) El último 0 de terminación es también el primer 0 que inicia la siguiente bandera.
- (c) La bandera de terminación de un frame es también la bandera de inicio del siguiente frame.
- (d) Se insertan dos banderas entre la bandera de terminación de un frame y la bandera de inicio del siguiente frame.

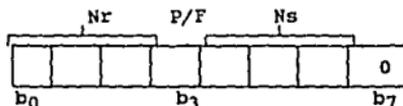
Si se transmite una dirección, está es siempre la del secundario. Si el primario la transmite, está diría "Este mensaje es para..." si el secundario la transmite, diría "Este mensaje es de..." El primario no tiene dirección. El secundario puede ser una terminal, un grupo y/o un mensaje para todas las direcciones. FFH es usado como dirección para todos. Si el primario envía información de dirección igual a FFH, todas las estaciones secundarias en la línea reciben la información. La 00H no es asignada a ninguna estación. Está es llamada "Dirección Vacía" y puede ser utilizada por el primario para fallas del sistema.

El Frame Check Sequence (FCS) es calculado usando CRC-16 (Cyclic Redundancy Check). El CRC es calculado sobre la secuencia de bits que conforman la bandera de inicio y el texto. CRC-16 genera 16 bits para detección de errores.

El campo de control tiene tres formas : Información, Supervisor y No-Numerado (Sin-Secuencia). El tipo de formato usado es determinado por los dos últimos bits significativos del campo:

b6	b7	
X	0	Información (Existe Texto)
0	1	Supervisor (No Existe Texto)
1	1	No-Numerado (Posiblemente con texto)

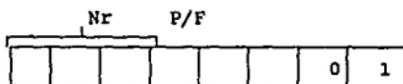
Formato de Información. La figura muestra el patrón de un campo de información. El bit 3 es el Poll/Final (P/F) bit. Si la transmisión es desde un primario a un secundario, este bit es un poll bit. Si $P=0$, el frame no es un poll y el secundario no es invitado a contestar. Si $P=1$, el frame es un frame de poleo y el secundario es invitado a responder después de recibir este frame. Si la transmisión es desde un secundario hacia un primario, este bit es un bit final. Si $F=0$, el frame es enviado por un secundario y no es el último frame y el primario no responderá. Si $F=1$, el frame enviado es el último frame que el secundario envía en esta secuencia y el primario debe contestar.



El Nr (número recibido) transmitido por el primario es relacionado con el Ns (número enviado) transmitido por el secundario; el Nr transmitido por el secundario es relacionado con el Ns transmitido por el primario. Si el formato de información es utilizado, el texto es enviado en frames numerados. El que envía identifica cual es el frame que va a enviar por Ns (número de 3 bits). Si Ns=010, el frame 2 está enviándose. Cualquiera que reciba la información transmite el Nr que identifica el número del siguiente frame esperado. Si el secundario transmite un Ns=2 y recibe un Nr=3, el primario esta enterado y recibio bien el frame Nr-1 y esta esperando recibir el frame 3.

Un máximo de 7 frames pueden ser transmitidos sin un llamado de confirmación. La confirmación es hecha por un P/F en 1. El enterado (Nr) puede ser hecho con un frame de información si se recibe el final y se tiene información para transmitirlo con un frame supervisor si no se tiene texto que transmitir.

Formato Supervisor. Es identificado por un 01 en los dos últimos bits. El secundario borra un RNR al enviar un frame de información con F=1 o un RR o REJ frame con F=0 o 1. El primario borra un RNR por enviar un frame de información con P=1 o un RR o REJ con un P=0 o 1.



b ₄	b ₅	
0	0	Ready to Receive (RR)
0	1	Not Ready to Receive (RNR)
1	0	Reject (REJ)

Formato No-Númerado. Si los dos últimos bits del el campo de control son 1, se trata de un No-Númerado. Como su nombre lo dice, estos frames son enviados sin número, es decir, el campo de control no tiene Nr ni Ns. La siguiente tabla muestra la configuración del No-Númerado.

Configuración Binaria		Mnemónico	Enviado por el Primario	Enviado por el Secundario	Permite Texto
b0	b7				
000	P/F	0011	UI	X	X
000	P	0111	SIM	X	
000	F	0111	RIM		X
100	P	0011	SNRM	X	
000	F	1111	DM		X
010	F	0011	RD		x
010	P	0011	DISC	X	
011	P/F	0011	UA	X	
100	F	0111	FMRM	X	X

UI	Unnumbered information (NSI-Nonsequence Information)
SIM	Set Initialization Mode
RIM	Request Initialization (RQI-Request Initialization)
SNRM	Set Normal Response Mode
DM	Disconnect Mode (ROL-Request On-Line)
RD	Request Disconnect (RQD-Request Disconnect)
DISC	Disconnect
UA	Unnumbered Acknowledgment (NSA-Nonsequenced Acknowledgment)
FMRM	Frame Reject (CMDR-Command Reject)

RIM es transmitido por el secundario para notificar al primario la necesidad de un comando SIM, éste es enviado al secundario con el propósito de inicializar el nivel de función. El primario y secundario inicializan el Nr y Ns con este comando. El secundario se queda esperando un UA en modo de respuesta o en modo desconectado, el secundario puede transmitir y recibir solo comandos no-números, en este modo el secundario esta fuera de línea. En el modo normal de respuesta el secundario es capaz de transmitir y recibir frames de información, supervisores o no-números. El secundario no puede cambiar el modo normal de respuesta o el modo desconectado por si solo pero puede solicitarlo al primario. Si asumimos que inicialmente el secundario esta en modo desconectado y que el primario envía un frame de información al secundario, éste recibe pero no puede atenderlo y entonces el secundario responde con un frame no numerado DM, que el primario interpreta como "Estoy en modo desconectado y no puede recibir frames de información", el primario entonces transmitirá un frame SNRM el cual pone al secundario en modo normal de respuesta. Cuando el primario recibe un UA del secundario, éste entonces retransmite el(los) frame(s) de información. Si el secundario esperaba recibir el modo desconectado después de recibir el mensaje del primario, debe regresar un frame supervisor para dar al primario un "Numbered Acknowledgment" con el bit F=0. El siguiente frame seria un no-número RD. El primario respondería con DISC, el cual regresaría al secundario para ponerlo en modo desconectado. El secundario esperaría regresar un UA.

Para transmitir FRMR, el secundario debería estar en modo normal de respuesta. El FRMR indica al primario que el frame recibido por el secundario es inválido. Un frame puede ser inválido por las siguientes razones :

1. El campo de control no pudo ser implementado por el secundario.
2. El campo de información es muy largo para almacenarse en el buffer de la estación receptora.
3. El campo de control recibido no puede tener un campo de información en este frame.
4. El Nr recibido del primario es inválido

El texto que viene con FRMR es fijado y usado para identificar la razón de por que el frame es inválido, el formato de un frame "reject" es el siguiente :

Bandera	Dirección	Control FRMR	Control del Frame Reject	Ns Nr FCS Bandera 0xxx0xxx wxyz 000
---------	-----------	--------------	-----------------------------	--

Ns y Nr son los valores presentes de los contadores en el secundario.

W = 1 Si el secundario recibió un comando inválido o si no lo puede ejecutar.

X = 1 Si un campo con información prohibida es recibido.

Y = 1 Si hay overflow en el buffer (campo de información demasiado largo).

Z = 1 Si el Nr recibido no concuerda con el Ns transmitido.

Los siguientes cuatro 0's después de z son de relleno para completar el byte.

Una vez que el secundario transmite un FRMR, éste no puede liberarse por sí solo de esta condición y repetirá el FRMR cuantas veces sea necesario hasta que reciba un comando DISC, SIM o SNRM los cuales desactivan la condición FRMR.

Estándar X.25

La recomendación X.25 fue desarrollada bajo los estándares del CCITT (Consultative Committee on International Telegraph and Telephone), en un esfuerzo conjunto de Canadá, Francia, Japón y U.S.A., emitida en 1980.

Se compone de tres niveles de conexión en el modelo OSI (Open System Interconnection): físico, enlace de datos y red. Tiene un conjunto de normas asociadas para la conexión de equipos asincrónicos (X.3, X.28 y X.29) y para la conexión con otras redes (X.75).

Una red de conmutación de paquetes X.25, es una red de comunicaciones de datos que usa la tecnología de conmutación de paquetes para efectos de transmitir los datos. Estos se encuadran en marcos (tramas) que contienen estructuras (paquetes) cuyo formato se ajusta a las especificaciones emitidas por el CCITT.

X.25 especifica las características de la interconexión ente el DTE (quien envía o recibe paquetes de datos) y el DCE (el nodo de la red que obra como entrada o salida de la misma). Estas características se detallan en tres niveles de procedimientos de control.

Nivel 1.

Especifica el uso de un circuito síncrono FDX, punto a punto que proveerá la vía para la transmisión física entre el DTE y la red. Este nivel es funcionalmente equivalente a la capa 1 de OSI. Se recomienda el uso del estándar CCITT V.24 (EIA RS-232C) en la interface física entre el DTE y un modem. Para el caso de utilización de un circuito digital, el ESTANDARD recomendado es X.21. Puede usarse el reemplazo del RS-232c, o sea el RS-449.

Nivel 2.

Describe el procedimiento de acceso al enlace, a ser usado para el intercambio de datos entre un DCE y un DTE. Este es correspondiente a la capa 2 de OSI se determina la utilización de la disciplina de línea HDLC y la clase de procedimientos de ISO para un sistema balanceado punto a punto, a éstos se les llama LAPB (Link Access Procedures Balanced). El uso de los procedimientos DLC asegura que los paquetes proporcionados por el nivel 3 se guarden en tramas HDLC y son confiablemente transmitidos entre el DTE y la red.

El procedimiento correspondiente al nivel 2 es ejecutado por módulos de software, tanto en el DTE como en el DCE.

Nivel 3.

Es el nivel más alto de la recomendación X.25 y especifica la manera en la cual la información de control y los datos del usuario se estructuran en paquetes. La información de control con del direccionamiento, está contenida en el encabezado del paquete (Packet Header) y le permite a la red identificar el DTE hacia el cual el paquete está destinado.

El X.25 define procedimientos que se usarán, entonces, en la interconexión de un DTE (que opere en modo de paquete) y el equipamiento de la PDN, usualmente llamado DCE.

La interface X.25 provee el acceso a los siguientes servicios que podrá proporcionar la PDN :

- 1 Circuito virtual conmutado (SVC:Switched Virtual Circuit).
- 2 Circuito virtual permanente (PVC:Permanent Virtual Circuit).
- 3 Datagrama (DG).

Un circuito virtual es una vía de flujo controlado, transparente y bidireccional entre un par de puertos físicos y lógicos. Realmente es un circuito físico compartido en parte, por muchas terminales a través del no uso de la técnica de multicanalización por división del tiempo, provista por la empresa transportadora. Un SVC asocia temporalmente y lógicamente dichos elementos y sólo ocupa un camino físico en el preciso momento de viaje de los datos.

Dado que es una conexión temporal, el DTE (que llama) emite un requerimiento de conexión hacia la red, que ésta analiza y autoriza (o no), estableciendo el enlace lógico con el destino requerido.

Un PVC es una asociación permanente entre dos DTE's la cual es equivalente lógico en una línea privada dedicada, punto a punto. De esta forma, no es necesario una llamada de requerimiento por parte de una de las DTE's.

Un DG, es un bloque de datos que contiene suficiente información de control en su interior, como para no necesitar el apoyo de otro tipo de mensaje, para efectos de lograr una transmisión confiable hacia el destino previsto.

El CCITT ha emitido nuevas recomendaciones sobre los estratos superiores del modelo OSI. Estas son:

- X.215, que especifica los servicios de la capa de sesión(5).
- X.214, que especifica los servicios de la capa de transporte(4).
- X.225, que especifica el protocolo de la capa de sesión(5).
- X.224, que especifica el protocolo de la capa de transporte(4).
- X.121, que especifica el plan de numeración de las redes públicas de datos.

DESEMPEÑO

La definición de parámetros para medir el desempeño de la red lo realiza el departamento de comunicaciones, ya que son los responsables de la operación del equipo. No interviene ninguna otra área para la definición de estos.

Para identificar condiciones problemáticas o anormales, tenemos los reportes de alarmas que aparte de avisar en las pantallas de los operadores existen impresoras en las que también aparecen. Se tiene tres tipos de alarmas:

- 1 Actuar de inmediato, se detiene la operación de la red (parcial o total)
- 2 Puede seguir operando la red, pero se corre el riesgo de una falla de tipo 1.
- 3 No existe riesgo, pero se debe dar seguimiento a esa falla.

La definición de parámetros se encuentra basada en la operación del banco. No se miden los parámetros que reflejan la calidad del servicio desde el punto de vista cliente.

El proceso de medición se lleva a cabo en forma automática, es decir, lo realiza el mismo equipo de comunicaciones (DCP : Data Communication Processor).

En la parte de monitoreo de la red, si se puede identificar cuales son los componentes que mas afectan a la operación de la red. Mensualmente se emite este reporte donde se especifica a que componente de la red corresponden las fallas que se presentaron en ese período. En nuestro caso, la mayoría de las anomalías se presentan por problemas en los modem's (microondas) y los equipos terminales (cajeros automáticos, equipo macro y mini, terminales de sucursal, etc).

En éste caso no se utiliza ningún método estadístico, ya que este tipo de información tiene que considerar toda la información para sus reportes, y nosotros para validar esa información utilizamos el método de muestreo por criterio.

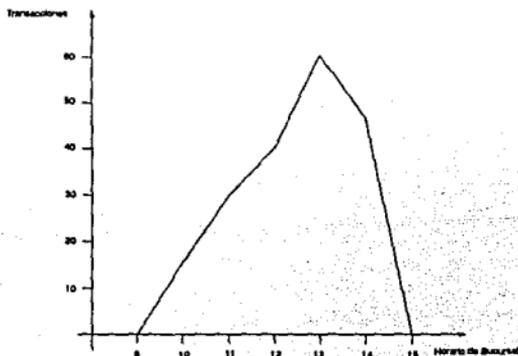
A continuación evaluaremos la información proporcionada (reportes y estadísticas), además de evaluar los parámetros que se utilizaron.

Para tener los elementos necesarios de disponibilidad, capacidad de transmisión, tiempo de respuesta y utilización de la red; se solicitó una copia de los reportes y estadísticas que se emiten actualmente y que tienen como objetivo informar lo antes mencionado. Con la finalidad de que nosotros podamos conocer los parámetros que se están utilizando.

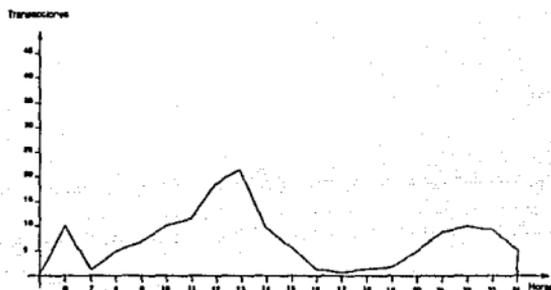
De lo que se observó, sólo se tiene lo siguiente: reportes que relacionan las transacciones que se operan en cada terminal. Entendiendo por terminal, cada cajero automático, terminal de sucursal, terminal de servicios especiales, etc. y como transacción cada una de las operaciones bancarias como son: consultas, retiros, depósitos, transferencia de fondos, pagos de servicios, pagos de tarjeta de crédito, etc.

De antemano conocemos que todas estas transacciones viajan diferente número de veces a través de la red por lo que consideramos inadecuada la información que se esta presentando; sin embargo, esta información nos sirve para conocer las horas de mayor saturación de la red (horas pico).

PROMEDIO DE TRANSACCIONES EN SUCURSALES



PROMEDIO DE TRANSACCIONES EN CAJEROS AUTOMATICOS



De lo que se observa que la hora pico en sucursales es de las 13:00 a las 14:00 horas, y en los cajeros automáticos de 11:00 a 13:00.

Para conocer la diferencia que existe entre los reportes de transacciones de las sucursales contra las veces que realmente viaja una transacción a través de la red tenemos la siguiente tabla :

OPERACION	NUM. DE VECES QUE VIAJA A TRAVES DEL ENLACE SUCURSAL	CAJERO AUTOMATICO
Consulta	2	2
Retiro	4	4
Depósito	4	4
Pago. Serv	4	4
Traspaso	4	4
Pago. Tarj	4	4

A partir de esta diferencia se decidió realizar un muestreo de criterio ya que los reportes que nos presentaron son parciales, es decir, sólo se obtienen en algunas regiones, y a nosotros nos interesa todo el universo que en este caso son las 6 regiones. Este muestreo consistió en seleccionar 3 sucursales de cada región y 3 cajeros automáticos, por un mes. De esto se obtuvo lo siguiente :

REGION 1

Sucursal 1.

Ter-minal	Consultas	Retiros	Depositos	Pago de Servicios	Pago de Tarjeta	Otros	Total
1	640	483	327	218	194	46	1908
2	324	216	415	58	184	56	1253
3	419	320	124	173	20	44	1100
4	290	114	264	28	79	48	823
Total	1673	1133	1130	477	477	194	5084
Real	3346	4532	4520	1908	1908	776	16990

Sucursal 2.

1	648	391	448	65	224	50	1826
2	421	360	184	104	114	46	1229
Total	1069	751	632	169	338	96	3055
Real	2138	3004	2528	676	1352	1384	10082

Sucursal 3.

1	720	524	631	83	320	50	2328
2	524	216	480	70	84	44	1418
3	321	415	390	120	114	48	1408
4	406	114	76	24	52	44	516
Total	1771	1269	1577	297	570	186	5670
Real	3542	5076	6308	1188	2280	744	19138

REGION 2

Sucursal 1.

Terminal	Consultas	Retiros	Depositos	Pago de Servicios	Pago de Tarjeta	Otros	Total
1	390	520	270	104	127	54	1465
2	518	360	410	56	315	46	1705
3	410	220	114	127	64	48	983
Total	1318	1100	794	287	506	148	4153
Real	2633	4400	3176	1148	2024	592	13976

Sucursal 2.

1	620	390	451	210	310	52	2033
2	300	214	321	56	124	48	1063
3	394	156	362	81	56	54	1103
Total	1314	760	1134	347	490	154	4199
Real	2628	3040	4536	1388	1960	616	12416

Sucursal 3.

1	413	216	514	118	191	48	1500
2	312	194	131	190	56	52	935
3	114	216	191	118	84	46	663
Total	839	620	836	326	331	146	3098
Real	1678	2480	3344	1304	1324	584	10714

REGION 3

Sucursal 1.

Terminal	Consultas	Retiros	Depositos	Pago de Servicios	Pago de Tarjeta	Otros	Total
1	690	410	220	129	200	46	1695
2	314	362	253	89	163	52	1233
Total	1004	772	473	218	263	98	2928
Real	2008	3088	1892	872	1052	392	9304

Sucursal 2.

1	390	219	415	220	117	46	1407
2	484	390	293	58	216	58	1493
3	210	104	315	112	123	54	918
Total	1084	713	1023	390	450	158	3818
Real	2168	2852	4092	1560	1800	632	13104

Sucursal 3.

1	610	415	219	194	210	50	1698
2	0	0	0	0	0	0	0
3	810	315	510	215	310	56	2216
4	310	120	210	56	84	50	830
Total	1510	850	939	465	604	156	4744
Real	3020	3400	3756	1860	2416	624	15076

REGION 4

Sucursal 1.

Ter-minal	Consultas	Retiros	Depositos	Pago de Servicios	Pago de Tarjeta	Otros	Total
1	317	215	410	120	310	54	1426
2	515	395	264	193	56	50	1473
3	215	153	292	87	104	52	903
4	298	243	109	53	89	58	850
Total	1345	1006	1075	453	559	214	4652
Real	2690	4024	4300	1812	2236	856	15918

Sucursal 2.

1	563	415	363	235	363	56	1995
2	490	253	384	196	274	44	1641
Total	1053	668	747	431	637	100	3636
Real	2106	2672	2988	1724	2548	400	12138

Sucursal 3.

1	198	364	515	318	104	58	1557
2	396	518	310	58	56	50	1388
3	219	405	215	64	219	48	1170
Total	813	1287	1040	440	379	156	4115
Real	1626	5148	4160	1760	1516	624	14834

REGION 5

Sucursal 1.

Ter-mina	Consultas	Retiros	Depositos	Pago de Servicios	Pago de Tarjeta	Otros	Total
1	403	294	163	217	173	58	1308
2	510	415	390	68	104	54	1541
Total	913	709	553	285	277	112	2849
Real	1826	2836	2212	1140	1108	448	9570

Sucursal 2.

1	290	351	308	104	56	58	1167
2	315	104	56	190	415	44	1224
3	518	415	370	76	24	62	1465
Total	1123	870	734	370	495	164	3856
Real	2246	3480	2936	1480	1980	656	12778

Sucursal 3.

1	410	354	215	198	310	52	1539
2	593	419	298	104	59	44	1517
Total	1003	773	513	302	369	96	3056
Real	2006	3092	2052	1208	1476	384	10218

REGION 6

Sucursal 1.

Ter-minal	Consultas	Retiros	Depositos	Pago de Servicios	Pago de Tarjeta	Otros	Total
1	407	490	263	124	163	80	1527
2	598	363	204	58	315	44	1582
3	104	215	160	44	29	54	606
Total	1109	1068	627	226	507	178	3715
Real	2218	4272	2508	904	2028	712	12842

Sucursal 2.

1	618	338	417	380	216	58	2027
2	320	518	216	114	189	68	1425
Total	938	856	633	494	405	126	3452
Real	1876	3424	2532	1976	1620	504	11932

Sucursal 3.

1	715	518	419	315	198	70	2235
2	614	316	118	56	315	44	1463
3	315	104	215	18	118	56	826
Total	1644	938	752	389	631	170	4524
Real	3288	3752	3008	1556	2524	680	14808

Comparando el valor que realmente viaja una transacción contra el valor de los reportes tenemos lo siguiente :

334.18 %
330.01 %
337.53 %
336.52 %
295.68 %
345.83 %
317.75 %
343.21 %
317.79 %
342.17 %
333.82 %
360.48 %
335.90 %
331.37 %
334.35 %
345.67 %
345.65 %
327.32 %

Realizando operaciones obtenemos un promedio de : 334.17, lo que significa que por cada vez que se considera que viaja, realmente se realiza 3.34 veces.

Cajeros Automáticos

Región	Cajeros	Consulta	Retiros	Depositos	Pago de Servicios	Trasposos	Total
1	1	1800	1120	129	68	315	3432
	2	2100	1321	58	24	401	3904
	3	1600	1400	94	78	240	3412
Total		5500	3841	241	170	956	10748
Real		11000	15364	1124	680	3824	31992
2	1	1740	1300	114	67	140	3361
	2	2400	800	83	45	327	3655
	3	1500	1320	67	18	127	3032
Total		5640	3420	264	130	594	10048
Real		11280	13680	1056	520	2776	29312
3	1	1100	620	24	4	43	2041
	2	1674	1281	111	37	217	3320
	3	2100	1600	46	21	198	3965
Total		4874	3501	181	62	458	9076
Real		9748	14004	724	248	1832	26556
4	1	1340	1320	98	67	315	3140
	2	2600	1800	54	48	270	4772
	3	1750	1440	98	53	271	3612
Total		5690	4560	205	168	856	11524
Real		11380	18240	820	672	3424	34536
5	1	1530	1224	133	63	293	3243
	2	2120	1114	88	18	113	3453
	3	420	218	4	2	33	677
Total		4070	2556	225	83	439	7373
Real		8140	10224	900	332	1756	21352
6	1	1910	1131	93	64	312	3510
	2	2044	1310	124	28	167	3673
	3	1300	820	125	68	350	2663
Total		5254	3261	342	160	829	9846
Real		10508	13044	1368	640	3316	28876

Comparando nuevamente tenemos :

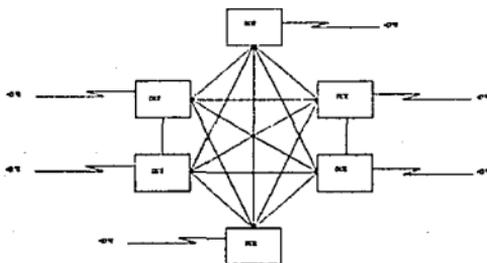
297.65
291.71
284.75
299.68
289.59
293.27

Realizando operaciones obtenemos : 292.77

De lo que concluimos que para las sucursales tenemos un 334.17 % extra de transmisiones o utilizations de un enlace y un 292.77 en enlaces de cajeros automáticos.

Lo anterior no significa que se utilizan de mejor forma a los cajeros automáticos sino que en estos se realiza mayor número de consultas que en una sucursal.

Como tenemos una red de este tipo



La información que se transmite de un DTE (Data Transmission Equipment) a un DCE (Data Communication Equipment), si viaja el número de veces que antes se menciono, pero la comunicación que existe de un DCE a otro no necesariamente es ese número, en este caso dependerá del protocolo que se esta utilizando (X.25), es decir, como organice la transición en los nodos.

Cabe mencionar que la mayoría de las transacciones que viajan van de un DTE a un DCE inmediato, ya que la función del banco es que sus cuenta habientes generalmente se mantienen en la región donde abrieron su cuenta; sin embargo, en el servicio de cajeros automáticos es más frecuente que un cliente que tiene su cuenta en Puebla quiera acceder su cuenta desde Monterrey o cualquier otro lado de la república.

Lo que significa que tenemos dos tiempos diferentes de utilización de los enlaces, uno sería el tiempo entre troncales y el otro sería de DTE a DCE o viceversa.

La utilización del enlace entre un DTE a un DCE es aproximadamente de un 44% (Es medido con el número de llegadas al DCE y la velocidad de los enlaces).

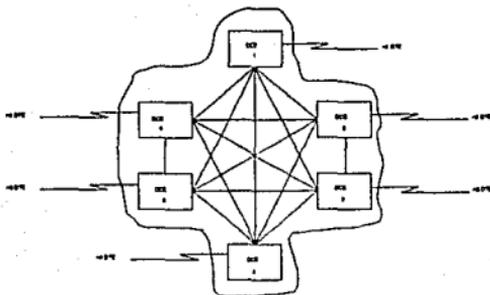
Para conocer la utilización de los enlaces entre troncales se tiene un software en el DCE que informa los paquetes que fueron enviados por cada nodo, así se suman el de los seis y como se conoce cuanto tiempo se tarda en transmitir un paquete, se obtiene el tiempo de utilización de la red en las 24 horas. Se consideró este tiempo y no el de sucursal porque la red no se utiliza solo para cajeros automáticos o sucursales sino toda la operación del banco.

Si se transmiten en promedio 20 millones de paquetes por nodo, y se tiene la capacidad de transmisión de 1000 paquetes por segundo y un día tiene 86400 segundos. Tenemos una utilización del 23.14 % en los enlaces de un DCE a otro.

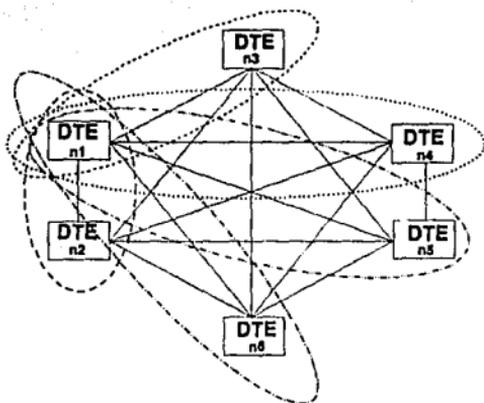
El tiempo que tarda en transmitir un paquete de un nodo a otro, varía si se tiene diferente medio de transmisión, algunos enlaces se tienen por satélite, microondas, radio o líneas privadas, todos éstos tienen características diferentes, lo que más nos interesa es la velocidad a la que esté transmitiendo. En nuestro caso es el satélite y como alterno microondas, durante el tiempo de la revisión no se requirió pasar de enlace satelital a microondas por lo que vamos a considerar la de satélite.

Para conocer la capacidad máxima de transmisión se cuenta con un software que realiza una simulación de situaciones críticas de la red, conociendo de esta forma a que porcentajes de saturación u ocupación de la red tenemos.

De este caso tenemos :



Antes de medirlo utilizando este software, se debe conocer la capacidad de almacenamiento de información (throughput), es decir, cuantos paquetes puede encolar un nodo. Lo ideal sería que para el nodo # 1 su capacidad fuera $N1$ (el número de DTE's conectados al nodo), y de esta misma forma los demás, si todos los DTE's conectados a ese nodo deciden hacer una petición a la red al mismo tiempo, de tal forma que este nodo pueda encolar todas esas peticiones, de lo contrario, no es tan problemático ya que un DTE puede transmitir o no, pero lo anterior no significa que el tamaño del "buffer" de almacenamiento sea la capacidad máxima de transmisión, finalmente como todos los DTE's están conectados a los DCE's, en los DCE's es donde se debe medir la capacidad máxima de transmisión de una red, que en nuestro caso fue medido con un software con que cuenta el Banco, en este software se definen todos los nodos con todos sus enlaces, es decir, si tenemos :

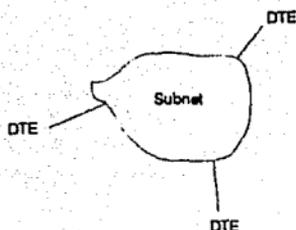


En este caso se observa como se comporta el nodo n_1 con respecto a que si todos los DTE's de otro nodo (n_2) quiere enviarle información a uno de los DTE's de n_1 y así con los demás nodos; n_1 con n_2 , n_1 con n_3 , n_1 con n_4 , n_1 con n_5 y n_1 con n_6 . El siguiente paso sería ver como se comportan los otros nodos.

Al finalizar esta prueba ya se tiene un criterio para saber que pasa con todos los nodos, como segundo ejercicio se puede observar que pasa con el n_1 si envían n_2 y n_3 , luego si a n_1 le envían n_2 , n_3 , n_4 , n_5 y n_6 .

El objetivo de esto es saber si la red se encuentra balanceada en los nodos principales, con esto se puede saber cual es la capacidad máxima de transmisión que en nuestro caso son 210 Kbps con una capacidad de almacenamiento (throughput) de 2600 pps (palabras por segundo). Si observamos la capacidad que el equipo ofrece, tenemos que la velocidad es de 64 a 256 Kbps.

Otro de los reportes que se nos entregaron nos muestra la disponibilidad de los enlaces de la red, antes de medir la disponibilidad de la red, se debe conocer si todos los enlaces que forman la red cuentan con un alterno, ya que si no es así la disponibilidad puede tenerse desde un 30.0% hasta un 99.9% dependiendo de cuantos enlaces no tengan un alterno. Siempre que se diseña una red, nos interesa que tenga una disponibilidad del 98.0 a 99.9%



En nuestro caso todos los enlaces que forman la parte de transporte cuentan con un alterno lo que nos confirma los resultados obtenidos en los reportes, una disponibilidad del 99,9%.

Tiempos de respuesta para transacciones interactivas

Los tiempos de respuesta dependerán de :

Velocidad de los enlaces

Horas pico

De prioridades dependiendo de la aplicación.

Tipo de transacción

Para este caso dividimos en cuatro situaciones dependiendo de la utilización

A	12:00 a 15:00
B	9:00 a 12:00
C	15:00 a 22:00
D	22:00 a 9:00

La A será la de mayor utilización y la D la de menor.

Para A (12:00 a 15:00) tenemos que el tiempo de respuesta es de : 10 seg.

Para B (9:00 a 12:00) de : 6 seg.
 Para C (15:00 a 22:00) de : 2 seg.
 Para D (22:00 a 9:00) de : 0.1 seg.

Con la finalidad de dar elementos al siguiente punto de evaluación (Eficiencia de la red), se investigó el número de transacciones que se realizaron durante un mes en toda la red (6 regiones), el cual se utilizará para obtener el costo promedio por transacción, únicamente se consideran las transacciones de cajeros, sucursales y terminales administrativas.

Región	Número de Cajeros Automáticos	Número de Terminales en línea	Número de Transacciones	
			Cajeros	Sucursales
1	18	258	68534	419524
2	10	63	41312	118615
3	15	55	57389	94543
4	8	45	29876	89543
5	18	51	84675	125679
6	5	31	16386	67504
		Total	298172	915408
		Total	1,213,580.	

EFICIENCIA

Los parámetros de eficiencia que son relevantes para la operación de la red son todos aquellos gastos que se cargan a ese departamento.

La función del departamento de planeación es: analizar una posible reconfiguración de la red, la evaluación periódica de alternativas tecnológicas y nuevos productos.

No se emite ningún reporte de eficiencia de la red por lo que nosotros recolectaremos la información para obtener los costos.

A continuación se muestran los parámetros y procedimientos utilizados.

En esta parte describiremos como se obtienen los costos promedio por transacción y por terminal conectada a la red para obtener la información de costos de la red se requirió apoyo de varias áreas como son: Recursos humanos, departamento de compras, pagos de servicios y contabilidad. De lo que se obtuvo lo siguiente:

Sueldos. Para esto se solicito al departamento de recursos humanos el importe de los sueldos del personal de comunicaciones de las 6 regiones, esto se solicitó de esta forma con la finalidad de que nos proporcionaran no solo lo que se recibe en nómina, sino que se contemple prestamos, aguinaldo, vacaciones, etc.

Región	Núm. Empleados	Importe
1	58	\$ 220'463,415
2	41	163'218,379
3	17	71'000,015
4	34	95'000,918
5	24	49'068,521
6	19	58'873,019
	Total	\$ 657'624,267

Gastos Administrativos. En el banco existe un área que se encarga de realizar los pagos de energía, agua, teléfono, rentas o utilización de locales, gastos de limpieza y aire acondicionado. De esto nos entregaron un total por cada región.

Región	Importe
1	\$ 224'973,264
2	168'729,948
3	123'735,295
4	73'116,310
5	101'237,968
6	134'983,958
Total	\$ 826'776,743

Esta misma área se encarga de realizar el pago de las frecuencias de satélite, radio y microondas que se tienen contratadas.

Para radio tenemos 40 pares de frecuencias (80 frecuencias) asignadas con cobertura a nivel nacional, es decir, se puede utilizar la misma frecuencia en diferentes partes de la república cuyo costo anual asciende a \$ 5,420'000,000 y la parte proporcional mensual es de \$ 451'667,000

Para los enlaces vía satélite tenemos un pago mensual por \$ 45'394,640.

Para los enlaces de microondas se paga mensualmente por 58 enlaces \$ 59'364,108.

Se considera que el 20 % de utilización de los equipos macro y mini es para comunicaciones, por lo que se toma el mismo porcentaje de la amortización mensual de estos equipos :

Región	Unisys	IMB/S38
1	(1) \$ 8'069,308	(5) \$ 17'560,590
2	(1) 8'069,308	(4) 14'048,472
3	(1) 8'069,308	(4) 14'048,472
4	(1) 8'069,308	(3) 10'536,364
5	(1) 8'069,308	(3) 10'536,364
6	(1) 8'069,308	(2) 7'024,236
Subtotal	\$ 48'415,848	\$ 73'754,478
	Total	\$ 122'170,326

Para la parte de cajeros automáticos, impresoras, modems, controladores de sucursal, encriptores, equipo de mantenimiento y control, terminales de monitoreo, multiplexores, FEP's y DCP's, se consideran los siguientes gastos por concepto de amortización (algunos ya depreciados totalmente) \$ 9'000,000.

Gastos por enlaces vía satélite, se considera únicamente el equipo utilizado : antena 3.7, modem satélital, equipo de switcheo, rack y amplificador de onda progresiva, cuyos gastos ascienden a \$ 121'203,780.

Gastos por enlaces de radio, en este caso se consideran los radios, torres y las antenas que ascienden a :

Región	Radios	Antenas	Torres	Importe
1	20	16	11	\$ 6'323,333
2	16	12	9	5'266,084
3	16	12	9	5'266,084
4	10	8	6	3'224,066
5	12	10	7	3'877,491
6	6	5	4	2'001,145
		Total		\$ 25'958,203

Mantenimiento de Equipo, como todas las compras se concentran en la Región 1 de esa misma forma se concentran los contratos de mantenimiento que son de dos tipos :

Mantenimiento correctivo que cubre :

- Terminales On-line
- Impresoras Sucursales
- Modems
- Controlador de Terminales
- Equipo de Monitoreo y Control
- Encriptores
- Multiplexores

Este equipo tiene mantenimiento correctivo por que se cuenta con equipo de respaldo, en el mes que se tomó la muestra estos gastos ascendieron a \$ 58'343,121.

Mantenimiento Preventivo y Correctivo, este cubre a :

FEP's
 DCP's
 Cajeros Automáticos
 Equipo Satélital
 Equipos IBM (parte proporcional)
 Equipos Unisys (parte proporcional)

En este caso los contratos son anuales y la parte proporcional es \$ 85'601,764.

La parte que corresponde al equipo de radio tiene garantía.

Resumiendo tenemos lo siguiente :

Sueldos	\$ 657'624,267
Gastos Administrativos	826'776,743
Frecuencias	
Radio	451'667,000
Satélite	45'394,640
Microondas	59'364,108
Depreciación	
Equipo Macro y Minis	122'170,326
Equipo satélital	121'203,780
Equipo radio	25'958,203
Equipo General	94'000,000
Mantenimientos al equipo	143'944,885
Total	\$ 2,548'103,952

Anteriormente observamos que las transacciones que se habfan realizado en el mes fueron : 1,213,580, luego entonces tenemos

$$\begin{aligned} \text{Costo promedio por transacción} &= 2,548'103,952 / 1'213,580 \\ &\quad \text{[pesos/transacciones]} \\ &= \$ 2,117 \end{aligned}$$

EVALUACION DE LA ADMINISTRACION

Al hablar de la administración de la red de telecomunicaciones, es importante mencionar las facilidades que nos brinda el S.O., algunas de las herramientas más importantes son las siguientes : Nos brinda la oportunidad de conocer que claves se encuentran en sesión, que procesos se están ejecutando en línea y en batch, el estado de las colas de impresión, quien tiene asignados los archivos activos, el estatus de las unidades de cinta y una herramienta para saber que se encuentra ejecutándose, quien está asignado en una terminal o preguntar por un usuario específico.

Por otro lado se cuenta con un equipo IBM en la zona central que prueba en forma continua todos los puntos de la red; este monitoreo es exclusivo para verificar que no existan problemas en el medio de comunicación. Para monitorear los puntos extremos de la red se detectan las diferentes configuraciones (direcciones) de los DCP's y FEP's, al conocer las direcciones de los puntos extremos se envían mensajes a cada uno de éstos puntos y se espera una respuesta, cuando no hay está, se envía nuevamente el mensaje y si no contesta se reporta este punto como un punto con posibles problemas.

En ocasiones se recibe la contestación pero no se recibe limpia lo cual indica que nuestra transmisión tiene ruido. En general se clasifican los enlaces de 3 formas : enlaces activos, enlaces con ruido y sin enlace.

Cuando se detecta una falla, lo primero que se hace es entablar comunicación telefónica con el personal encargado del punto con falla y se pregunta si se ha detectado alguna anomalía en el equipo, si dice que todo está bien se procede a checar la configuración del equipo de comunicaciones, y si también está bien se conecta un equipo para verificar las señales, esto sería siempre con un equipo terminal (DTE), si no se detecta nada se trata de hacer la conexión lo más directo que se pueda, por ejemplo, si tenemos un radio-modem conectado a un multiplexor y del multiplexor varias terminales, conectamos una terminal directa al radio-modem y así sucesivamente vamos recortando hasta detectar la falla.

A todas las fallas detectadas por el sistema o las reportadas por el personal se les asigna un número consecutivo para poder darle seguimiento, y se archivan cuando son corregidas.

En muchas ocasiones se reporta o detecta un problema y al dar seguimiento a éste se detecta que la falla del equipo es por falta de corriente, ya sea por que lo desconectaron por error o bien por que se funde un fusible, cuando es la segunda causa se hacen lecturas de corriente para verificar si no existe algún problema con la energía suministrada.

El equipo dedicado al monitoreo depende directamente de una oficina de la gerencia de telecomunicaciones, la cual se encarga también de coordinar los cambios a las configuraciones.

Como ya lo mencionamos el equipo monitorea todos los puntos en forma constante, pero en ocasiones cuando hay mucha demanda se desactivan ciertos sectores para disminuir el tráfico y dar prioridad a las aplicaciones; en otras ocasiones, cuando se reporta una anomalía en alguna parte se le da prioridad a ese sector para que sea monitoreado más eficientemente, esto se hace por medio de software, bloqueando las direcciones correspondientes para que el equipo de monitoreo las ignore.

Cuando el sistema detecta una falla manda a la impresora y a la pantalla del operador un mensaje (alarma) y actualiza una bitácora de fallas. Los mensajes impresos se archivan y la bitácora se actualiza hasta que la falla es corregida.

En general en el Banco cuando una información ya no es relevante se archiva en cajas y se manda a un almacén con una forma que indica el contenido y fecha de destrucción.

Existen diferentes tipos de reportes estadísticos como son : tiempo de respuesta, utilización de los recursos de la red y usuarios conectados en un instante determinado.

Los diferentes usuarios se identifican por su clave que esta formada por la clave del departamento (3 posiciones) y la identificación del usuario (3 posiciones).

Al consultar los usuarios en sesión existe una opción para obtener información adicional del usuario como es nombre, ubicación y fecha de alta de su clave, por lo que nunca se tiene problema para identificar algún usuario.

En la actualidad se considera que estamos en un 35% de la capacidad máxima de la red, lo cual nos da una tranquilidad para plantear nuevos proyectos, pero como se observó en eficiencia incrementa el costo por transacción.

Para solicitar un servicio al departamento de telecomunicaciones se manda requisición, en la cual se detalla el servicio. Esto es cuando son cosas sencillas o menores. Cuando se trata de cosas mayores como plantear un nuevo enlace, se lleva al cabo mediante una junta con el área interesada y se evalúa en la gerencia de telecomunicaciones, cuando se aprueba, se le da seguimiento, es decir, se abre un "file", donde se archivan las minutas de la juntas, presupuestos y documentos en general. Cuando son servicios sencillos como mantenimientos, se le da un número de requisición de trabajo y se asigna a un empleado o algún proveedor que trabaja para el Banco.

No existe ninguna estrategia que plantee una visión de cómo evolucionaría la arquitectura de control con los avances tecnológicos.

Como ya mencionamos, los usuarios se clasifican por grupos, éstos, por ejemplo, pueden ser por oficinas o gerencias. Una oficina de captura de datos ó una sucursal pertenecen a un grupo donde únicamente se tienen los derechos de ejecutar procesos y no tienen ningún derecho de borrar. Una oficina de desarrollo tiene los derechos de borrar y crear datos en una área de disco destinada para desarrollo, pero una vez liberado algún proyecto se pasa a una área de disco restringida en la que sólo una persona con nivel de operador puede modificarla, también existen herramientas para tener protección sobre proyectos e inclusive archivos por medio del software de redes con que se cuenta.

Cuando se tiene algún problema con un sistema, ya sea en "batch" o en línea, un usuario con clave de supervisor, puede dar privilegios a una clave para manejar la información, para poder solucionar el problema, si éste realmente es relevante para la operación de alguna área, esto no es muy frecuente, cuando se presenta por lo regular es porque se acaba de liberar un sistema o que se actualiza una nueva versión de software, por lo cual es necesario que las áreas involucradas asignen gente de respaldo en caso de problemas. Únicamente en estos casos relevantes es cuando se realizan funciones que no se tienen establecidas.

La gerencia de telecomunicaciones está organizada por diversas áreas (oficinas) que atienden diferentes aspectos de la red como son : la administración, el mantenimiento, la planeación y el desarrollo. Las funciones que realiza cada área están claramente determinadas pero en algunos aspectos tienen que actuar algunas en conjunto. En la gerencia no hay personas especializadas en algo, es decir, no se crea dependencia en una persona, por lo cual cuando alguien falta, existen otras personas que pueden hacer el trabajo, cuando por algún motivo hay una vacante, se hace una selección por medio del departamento de personal y entrevistas con gente del área de telecomunicaciones. El Banco sigue la política de cubrir las vacantes lo más pronto posible, si alguna área no pide al departamento de personal la selección de alguna persona para el área, automáticamente se cancela la plaza por considerarse no necesaria.

Existe un formato para pedir trabajos al área de telecomunicaciones y el área administrativa se encarga de turnarlos a la oficina correspondiente, aunque en algunos casos se requiera la intervención de más de una oficina, pero todas estas requisiciones las controla el área administrativa, y las archiva cuando el trabajo ha sido concluido

Cada quince días hay juntas, donde se exponen los adelantos en los proyectos, los proyectos nuevos y las cosas que son relevantes, al día siguiente de la junta se entrega a todos los asistentes una copia de la minuta y el gerente de telecomunicaciones se encarga de archivar el original. Por lo regular en estas reuniones se fijan metas a corto y largo plazo, y también se da revisión a estas metas planteadas con anterioridad.

No existen por escrito las políticas y procedimientos de como se debe llevar la administración del área; sin embargo, existen políticas generales que actúan en todo el Banco

No existe un entrenamiento especial para la personas que se integran al área; sin embargo, se cuenta con algunos manuales de operación que se sugiere leer, por otro lado el jefe de la oficina se encarga de dar una introducción de el trabajo que se desarrolla en el área, y se recomienda bibliografía de la existente en el área. Cuando una persona es de nuevo ingreso a la institución, el área de personal se encarga de dar una plática de las políticas y procedimientos del Banco.

Cuando un empleado se da de baja, se le recogen las llaves que se le hayan proporcionado así como su credencial de empleado. Por otro lado el jefe del área se debe de encargar de pedir la baja de la clave y se recomienda cambiar los "passwords" que él conocía.

En el Banco existen un área de capacitación, la cual se encarga de planear y coordinar diferentes tipos de cursos, los cuales van dirigidos a diferentes áreas, por otro lado cada área puede solicitar algún curso especial para un grupo de empleados o para un sólo empleado, en el plan de actividades anual nunca se incluyen cursos, pero cada empleado puede sugerir algún curso cuando así lo desee.

En todas las actividades que se desarrollan en el área se da libertad a los analistas de actuar en sus proyectos, pero para realizar una prueba que requiera más recursos, como por ejemplo, personal de captura con horas extras, estas deben ser autorizadas por el subgerente del área; y cuando un proyecto a sido liberado y se requiere hacer una modificación se requiere una autorización para poder actuar y se distribuye una copia de la autorización a todas las áreas que intervienen en el sistema.

En la descripción de actividades semanales o mensuales no se incluye el puesto que ocupa ni las responsabilidades de las personas, únicamente se escribe el nombre del responsable.

En cuanto al tiempo extra solo se autoriza cuando son pruebas fuera de horario o en días festivos, pero en general para las personas del área rara vez se les autoriza tiempo extra. El subgerente que es el encargado de autorizar el tiempo extra, se encarga de analizar junto con las personas interesadas en hacer la prueba el tiempo y las personas que se requieren.

En cuanto a las vacaciones de los empleados, en el Banco se planean las de cada año a fines del año anterior y se organizan por oficinas, el procedimiento es el siguiente : se pide a los empleados con mayor antigüedad que marquen los días que tienen planeados tomar vacaciones y se va pasando el calendario de empleado en empleado hasta el que tenga menor antigüedad, pero, cada empleado debe tomar en cuenta no encimar días con otro empleado; sin embargo, como es una área operativa nadie respeta sus días.

En cuanto a la promoción de los empleados, en el Banco para admistrar a los empleados existen niveles y dependiendo de estos niveles es el sueldo que persive cada uno. Cuando existe capacidad para dar aumentos, los jefes de cada área pueden pedir algunos niveles para los empleados que hayan demostrado empeño y buenos resultados, para proceder se debe anexar un escrito donde se describa las actividades que desarrollo la persona. La propuesta de niveles es inicializada por el subgerente del área y autorizada por el director del área.

Existen en el Banco políticas para evaluar a los empleados semestralmente, el encargado de hacer las evaluaciones es el jefe del área, estas evaluaciones son confidenciales y los empleados no tienen acceso a ellas.

Como ya lo habíamos mencionado se lleva una bitácora de los problemas de operación del sistema y también se llevan estadísticas de la eficiencia del equipo.

Existe un área específica para hacer las compras donde tienen un directorio de los proveedores, el cual incluye el nombre del proveedor, representante, teléfono, descripción del producto o servicio y descuento (aproximado).

En cuanto al mantenimiento del equipo se tienen contratadas varias empresas, como IBM y Unisys para dar mantenimiento a sus equipos macros y minis, otras compañías dan mantenimiento a cajeros, equipo de telecomunicaciones y micros. En general se tiene dos tipos de contratos, uno de mantenimiento preventivo que se les da a todo el equipo en forma periódica y un contrato correctivo, para este segundo se tiene contemplado para todos los días del año a cualquier hora. Una oficina del área es la encargada de llevar el control de los mantenimientos preventivos al equipo y también de recibir los reportes de fallas de equipo para turnarlo a las personas o compañías correspondientes, así como dar seguimiento a todas las fallas hasta que estas estén solucionadas.

La frecuencia de los mantenimientos preventivos depende del equipo, por ejemplo, los equipos macros junto con sus FEP's son revisados en forma bimestral, las terminales y micros son revisadas dos veces al año, y así dependiendo del equipo, se lleva un control donde se indica la fecha de mantenimiento. La oficina encargada del mantenimiento también se encarga de renovarlos. Cuando alguno de los contratos desea ser modificado en alguna de sus cláusulas, éstas son analizadas y aprobadas en juntas. Además, todo contrato antes de ser firmado pasa a una área legal para que le den el visto bueno.

Únicamente los equipos macro se encuentran asegurados, contra pérdida total. Este contrato tiene un manejo muy especial por la importancia de los equipos con que se cuenta.

El área donde se encuentra el equipo de comunicaciones, es un área restringida, donde únicamente pueden entrar las personas autorizadas, el acceso se controla por medio de torniquetes que identifican las credenciales con cinta magnética y aparte hay policías que están resguardando la entrada. En caso de que alguien desee entrar sin credencial autorizada o por olvido de la credencial, debe traer un pase autorizado por el gerente del área. Para las personas o compañías que deben tener acceso para dar mantenimiento se gira un memorándum a la gerencia de seguridad, en donde se especifican los nombres de las personas y de que compañía vienen y se especifica las fechas en que han de realizar sus labores.

No existe ningún plan de capacitación formal para el uso del equipo; sin embargo, se cuenta con una gran bibliografía para consulta y autocapacitación (manuales de operación).

Existen algunas normas institucionales para el uso del equipo de cómputo y telecomunicaciones, las cuales comprometen al personal a hacer buen uso del equipo para fines del trabajo.

EVALUACION DE REQUERIMIENTOS FUTUROS

Es difícil tener un plan maestro para el desarrollo de la red de comunicaciones, esto es por que depende principalmente del desarrollo económico que tengan las distintas regiones, pero se tienen diferentes proyectos de acuerdo a las necesidades actuales y a los crecimientos inminentes, es decir, se sabe en que lugares se requiere una sucursal nueva, o más cajeros automáticos, lo que no cambia en esencia nuestra configuración de red actual; sin embargo, en la región central y norte del país se está viendo la necesidad de realizar algunos cambios que en un futuro no lejano se tienen que dar, es decir, que estas regiones tienen que ser divididas en dos. Pero como ya lo mencionamos es difícil determinar cuanto tiempo se va a requerir, pero ya se esta contemplando. También influyen mucho los planes institucionales que se tengan, puesto que en el Banco se esta enfocando a la calidad de los clientes no a la cantidad.

Por otro lado existen otros planes que no solo son los de expansión sino los de actualización, entre los que destacan la modernización de los cajeros automáticos y la introducción de equipos más modernos para no estancarse y conformarse con lo que se tiene.

Estos planes futuros no solo incluyen, expansión y actualización de equipo sino también requerimientos de personal nuevo y aparte una investigación constante de los nuevos productos tanto de software como de hardware. Para esto último se tiene una oficina en la gerencia de informática dedicada únicamente a la investigación de nuevos productos; cuando se decide que le conviene al Banco adquirir un producto se hace un plan de implantación en caso de que sea nuevo, o un plan de actualización en caso de que se tengan versiones anteriores.

Dentro del Banco existen fechas únicamente para los planes a corto plazo (no mayor de 2 años). Para los planes a largo plazo se tiene contemplado pero no se define hasta que este dentro del rango del corto plazo.

En cuanto a la actualización de planes de trabajo, existe una comisión permanente de analistas encargados de revisar los planes y darles seguimiento a través de las oficinas involucradas. Esta comisión también se encarga de revisar el comportamiento general del área de informática en la que se encuentra la gerencia de telecomunicaciones, en general lo que revisan son inquietudes generales, sueldos y estadísticas generales del personal de esta área.

Esta comisión está integrada por gente de diferentes áreas, pero a su vez se divide como es el caso de la comisión de informática que está compuesta en su mayoría por gerentes, jefes y analistas del área de informática y comunicaciones.

También algunas personas del departamento de auditoría toman parte en estas asambleas, en las cuales se designa a una persona como presidente de la asamblea quien es la encargada de llevar las mismas, así mismo se cuenta con una persona encargada de hacer la minuta, que se distribuye a todos los asistentes.

Dentro de los planes de compra de equipo destacan la compra de nuevos cajeros que se salen de la línea tradicional, es decir, que tienen otras funciones de las que actualmente tienen, también nuevas terminales para los cajeros de las sucursales, así como equipo en general que se tiene que sustituir (modems, multiplexores, etc.). Para la adquisición de este equipo se manda una requisición de compra al departamento de compras con las especificaciones del equipo, y este departamento se encarga de obtener la mejor cotización y hacer la compra.

Año con año se pide a todos los departamentos de la gerencia de informática y telecomunicaciones hacer una lista de los requerimientos de equipo de cómputo y comunicaciones para el siguiente año, cuando se tienen las listas el comité se encarga de analizarlo y autorizar las compras de acuerdo con el presupuesto que se tenga previsto.

Dentro de la gerencia de telecomunicaciones se cuenta con una serie de estándares, los cuales se toman en cuenta para la planeación, estos también son revisados en forma periódica para ser actualizados, la comisión de informática es la encargada de revisar y actualizar estos estándares. Cuando algún estándar requiere una modificación sustancial, es decir, que se cambia el estándar por otro, entra el área de implantación de proyectos para hacer el plan de implantación. Todas las áreas involucradas deben conocer los estándares y la comisión debe encargarse de actualizarlos cuando sea necesario. Cuando una acción se sale de los estándares esta es analizada por la comisión y si ésta determina que es inadecuada, entonces se realiza un plan para implementarse de la forma correcta. Las consecuencias de estas situaciones dependen de las razones que exponga el área.

INFORME DE AUDITORIA

Durante la revisión que se realizó a la red de telecomunicaciones, durante los meses de mayo a octubre del presente, a las seis regiones incluyendo zonas y plazas que constituyen toda la red de la institución, se evaluaron los aspectos de seguridad, desempeño, eficiencia y administración. Los puntos relevantes que arrojó la auditoría son los siguientes :

Equipo faltante

El inventario que se tiene en la región central no corresponde a los que se tienen en las seis regiones, el de la región central es el más confiable por estar basado en las adquisiciones de equipo a nivel nacional, aparte de ser la encargada de distribuir el equipo a las regiones; sin embargo, los inventarios de las otras regiones sí corresponden al que hay físicamente en cada una.

Las diferencias que se encontraron se describen a continuación : en la región No. 2 faltan 2 radios, 5 modems y un encriptador; en la región No. 3 faltan 2 encriptadores; en la región No. 5 faltan 2 radios, 2 modems y un encriptador; en la región No. 6 falta un modem y 3 encriptadores (en el anexo del informe final se define el equipo faltante por región). Estas diferencias las atribuimos a la falta de controles que se tiene sobre los inventarios, es decir, en algunas de las regiones sí se tiene un control adecuado, por ejemplo, se tiene el número de inventario, ubicación, responsable del equipo, estado (operando, mantenimiento, respaldo, etc.), fecha de último mantenimiento y próximo mantenimiento, por lo que nosotros recomendamos se lleve un estándar a nivel nacional.

Seguridad

Existen reportes donde se indica cuantos intentos de conexión inadecuados se tuvieron en la red, este reporte sólo se entrega al responsable de la configuración de la red cuando excede de 10 intentos en un día, para que éste le de seguimiento; sin embargo, nadie lo considera ni da seguimiento, lo que ocasiona que se presenten continuamente, ya que no se sanciona a quienes realizan este tipo de intentos.

No se cuenta con un software para la seguridad de la red, pero el sistema operativo proporciona algunos controles; sin embargo, no se cubre al 100% la seguridad, esto significa que se tiene algunos niveles de la red que no cuentan con seguridad.

Sólo se tienen encriptores para enlaces vía microondas a nivel nacional; por otra parte, en un muestreo que se realizó a los centros de control, se observó que se tiene el 60% de encriptores en modo de "seguridad" y el resto en "bypass" lo que consideramos inadecuado ya que el 40% de la información que se transmite en las sucursales y cajeros automáticos no está siendo encriptada, siendo un alto riesgo para el banco, ya que toda la información que se transmite es de tipo monetario.

Debido a que el enlace vía radio es el alternativo para líneas privadas y siendo los que dan servicio a las sucursales y cajeros automáticos, consideramos que los enlaces de radio también deben encriptar la información, de otra forma esto incrementa la transmisión de información no encriptada. Los encriptores cuentan con mantenimiento preventivo cada 6 meses el cual es insuficiente ya que contamos con equipo descompuesto continuamente y el equipo que se tiene de respaldo no cubre las necesidades de las regiones, lo que ocasiona se tenga que trabajar algunas sucursales sin encriptar.

Planes de contingencia

Todos los enlaces más importantes de la red (parte de transporte) cuentan con un enlace alternativo, y todo los equipos más importantes de comunicaciones como son los DCP's y FEP's tienen respaldo con la misma configuración del que se está operando, pero si por algún motivo se pierden los enlaces a una región, no se tiene ningún procedimiento por escrito. Para este caso recomendamos se analice la definición de un plan de contingencia que cubra esta situación (ya sea contratando una red pública o por medio de un convenio con una red privada).

Con el equipo de respaldo que se cuenta para la operación de la red (modems, encriptores, radios, equipo de monitoreo, etc.) no es suficiente para soportar la operación del banco, en este caso se sugiere tener más equipo de respaldo o mantenimiento preventivo para todos los componentes de la red.

No se tiene ningún procedimiento por escrito de la forma de apagar y encender el equipo. El año pasado, en la región No. 3 se presentó el caso de que se fue la luz y no entró de inmediato el no-break, lo que ocasionó que se apagaran todos los equipos, provocando la suspensión de la operación en toda la región por 4 horas.

Consideramos necesario hacer un simulacro de un incendio en el área del equipo de cómputo en las regiones de manera similar al que se hace en la región central, con la finalidad de que el personal conozca la forma de actuar en esta situación.

Las áreas de comunicaciones del interior de la república se encuentran abajo del nivel del suelo, lo que ha provocado, en las regiones 3 y 5, en los últimos dos años inundaciones considerables, por lo que recomendamos se realice un estudio por personas expertas para resolver esta situación, además de capacitar al personal para saber que hacer en estas situaciones.

Desempeño

Los aspectos más importantes que se observaron sobre desempeño son los siguientes :

Como la hora pico en sucursales es de 13:00 a 14:00 y en los cajeros automáticos es de 11:00 a 13:00 horas, se recomienda no realizar procesos que puedan aumentar la saturación de la red, esto es con la finalidad de poder ofrecer un mejor servicio, ya que los tiempos de respuesta en estas horas se incrementan considerablemente.

La utilización de la red para la parte de transporte es un 23.4 % y en la parte de transmisiones de DTE a DCE un 44.0 % aproximadamente. Como una red no se debe de tener saturada al 100 % sino a un 80 % podemos decir que para la parte de transporte no se utiliza un 56.6 % y en la parte de equipos terminales de un 35.6 %. De lo anterior podemos concluir que se cuenta con capacidad para poder incrementar equipos terminales o agregar más servicios a la red.

En la disponibilidad de enlaces en la parte de transporte es del 99.9 %, lo que significa que no se tienen problemas para tener acceso a la red, esto no implica que durante las 24 horas del día todos los enlaces están disponibles, únicamente se está hablando de la parte de transporte.

La capacidad de transmisión en los nodos es de 64 a 256 kbps; sin embargo, actualmente se cuenta con equipo que pueden llegar a transmitir hasta 64 Mbps por lo que sería conveniente analizar las opciones que brinda la tecnología actual, para que el día de mañana no se cuente con una red obsoleta.

El tiempo de respuesta en transacciones interactivas (consultas, retiros, depósitos, etc.) es de : 0.1, 1, 6 y 10 seg. Para este caso se recomienda realizar un estudio del tiempo que toma el acceso a los archivos de autorizaciones ya que es en este proceso donde se emplea la mayor parte del tiempo total de una transacción donde se ocupa la mayor parte del tiempo total de una transacción interactiva.

Eficiencia

El costo promedio de transacción es de \$ 2,117.00 pesos, este costo se obtuvo considerando todos los gastos que realiza el departamento de comunicaciones. En nuestra opinión este costo es adecuado ya que se ofrece un servicio a nivel nacional y en tiempo real, lo cual permite estar a la vanguardia en servicios bancarios y ofrecer grandes facilidades a los clientes. Adicionalmente, por la tecnología que se emplea y la disponibilidad que se tiene, se puede incrementar el número de transacciones sin aumentar prácticamente ningún gasto, lo que en el futuro hará que se disminuya sensiblemente el costo por transacción.

Administración

En la parte de monitoreo de la red, lo ideal sería que siempre los operadores se den cuenta de los problemas de la red, generalmente se lleva a cabo de esa forma, pero cuando llegan a existir varios problemas simultáneamente, éstos no son atendidos de inmediato por falta de personal en esta área, teniendo aproximadamente que un 20 % de las fallas no son atendidas en la forma adecuada sobre todo en el horario de sucursal.

En cuanto a las fallas que se presentan en la red, y que no son atendidas en el día en que se presentan, por lo regular ya no son atendidas, solamente que la falla sea de un enlace entre los equipos de comunicaciones (troncales). El procedimiento que nos mostraron es que a cada falla se le asigna un número consecutivo para darle seguimiento. Respecto a esta situación recomendamos que sí se atiendan todas las fallas que se presentan, de esta forma se reducirá el número de fallas de mayor riesgo.

Actualmente se tiene una saturación de la red de un 35 % de la capacidad máxima, lo que permite a esta área incorporar nuevos proyectos.

Los contratos de mantenimiento (tanto preventivo como correctivo) se encuentran centralizados en la región No. 1, esto se lleva al cabo así porque esta región se encarga de las compras a nivel nacional, por lo tanto lleva el control de cuales equipos están en garantía y cuales son los que deben tener un contrato de mantenimiento. Existe equipo que no tiene contratos como son los modems, controladores, terminales, que cuando se descomponen los envían a esta región, provocando una situación conflictiva, por el tiempo en que viaja el equipo, lo arreglan y se regresa a su origen es demasiado, teniendo que trabajar unas sucursales fuera de línea y en otros casos con muy pocas terminales. Para no continuar con esta situación recomendamos se solicite a los proveedores que tengan por lo menos un representante en cada región.

Cuando se contrata un nuevo empleado en el área de comunicaciones y por la cantidad de trabajo que se tiene, desde el primer día que se presenta, inicia sus labores, lo que consideramos con alto riesgo ya que no conoce los procedimientos que se llevan en el área y por error puede provocar una situación crítica en la transmisión de información, como podría ser apagar el equipo, tirar enlaces de sucursales, intentar corregir una anomalía de un enlace que está operando correctamente, etc.. A este aspecto recomendamos se implemente un programa de capacitación para nuevos empleados (tanto la parte bancaria como la técnica).

Requerimientos futuros

Se recomienda estandarizar el tipo de terminales que se tiene en cada región, actualmente se tienen dos modelos lo que provoca un incremento en gastos tanto por capacitación al personal como por mantenimiento. Se puede tener una región con todo este equipo o desecharlo por completo.

Por la mala calidad que presentan las líneas telefónicas en el país se recomienda cambiar paulatinamente al servicio vía radio.

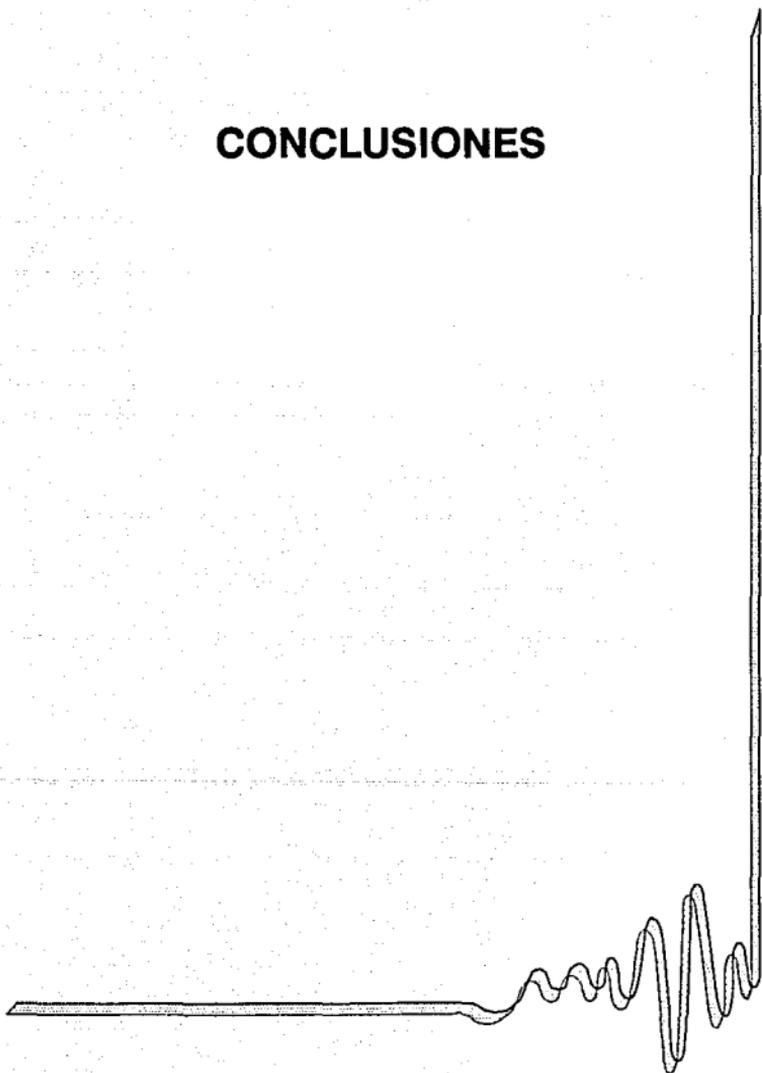
Actualmente no se tiene integrada la parte de voz en la red, teniendo capacidad para dar este servicio al mismo tiempo, no se debe olvidar que el objetivo principal de la existencia de la red es para la transmisión de datos.

ANEXO DEL INFORME FINAL

Región	Número de :		
	Rádios	Modems	Encriptores
1	24	112	105
2	18	55	53
3	18	56	53
4	12	42	40
5	14	44	41
6	7	27	25
Total	93	336	317
Total Central	97	344	324

Región con Diferencias	Rádios	Modems	Encriptores
2	20	60	54
3			55
5	16	46	42
6		28	28

CONCLUSIONES



CONCLUSIONES

El auditar una red de telecomunicaciones es un trabajo arduo, por lo cual en esta tesis, se definió una metodología sencilla, para ser utilizada por personas relacionadas con el área de ingeniería o auditoría sin tener que ser unos especialistas.

Durante el desarrollo de la tesis contemplamos que fue de vital importancia, definir los conceptos de las diferentes áreas involucradas; obteniendo como resultado una metodología afín a lo planteado inicialmente.

Al desarrollar la metodología pretendimos abarcar los diferentes aspectos relacionados con redes de telecomunicaciones; sin embargo, al ponerla en práctica nos percatamos que esta se debe de amoldar al caso en estudio, ya que en algunas redes sobran aspectos a evaluar.

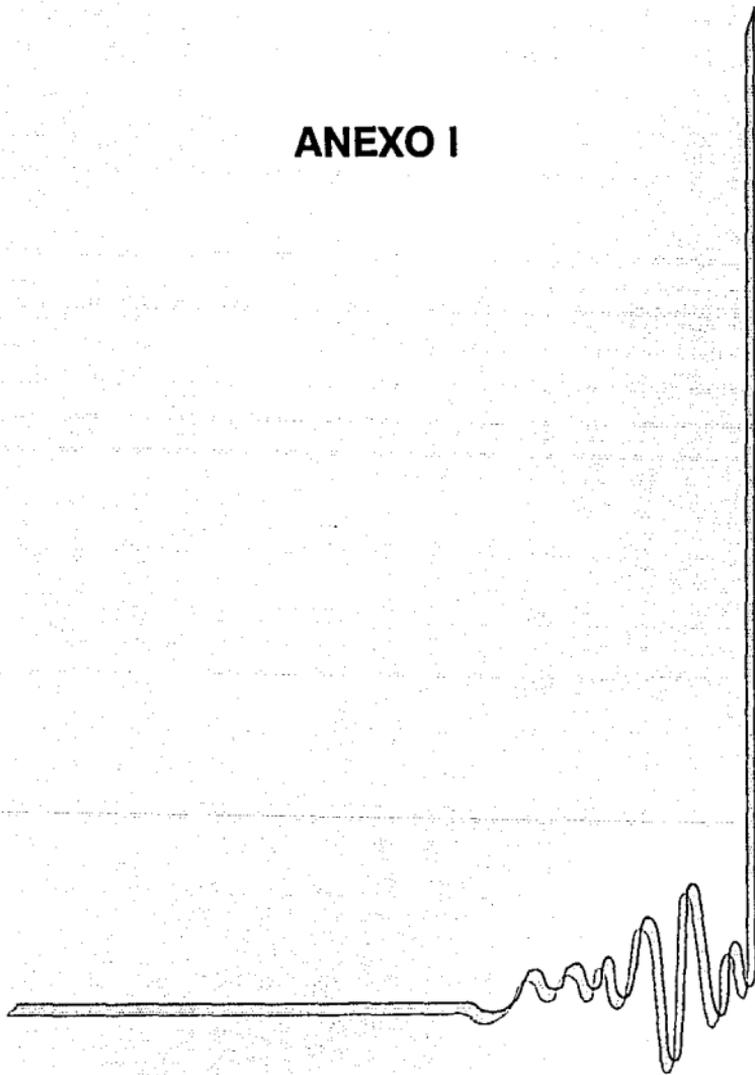
Como la metodología se diseñó en forma modular se brinda la posibilidad de evaluar únicamente algunos de los aspectos mencionado en ella, si así se requiere.

El aplicar esta metodología, nos permitió conocer la calidad de la misma; porque los resultados obtenidos fueron considerados para modificar o implantar políticas o procedimientos; además se ha diseñado un plan para dar seguimiento a cada una de las observaciones realizadas.

Finalmente consideramos que el objetivo inicial se ha cumplido satisfactoriamente.

Por lo expuesto, esperamos que esta metodología sea de utilidad a toda aquella persona interesada en este tema.

ANEXO I



ANEXO I

SERVICIOS QUE OFRECEN LAS SOCIEDADES NACIONALES DE CREDITO

CAPTACION DE RECURSOS

Cuenta de Ahorros.- Consiste en un contrato con la institución, en el cual una persona física o moral hace entrega de dinero, adquiriendo un interés anual capitalizable cada seis meses. Dicha persona podrá retirar parcial o totalmente su dinero solicitándolo a la institución.

Cuenta de Cheques.- El banco acepta, por parte del cliente, depósitos de dinero o documentos que se reciben salvo buen cobro, para ser acreditados en una cuenta de cheques. Los cuenta-habientes podrán disponer de los fondos en forma total o parcial, a la vista, mediante cheques que liberen contra su propia cuenta.

Cheque Certificado.- Son aquellos cheques que la institución declara que tienen suficientes fondos para cubrir el cheque a su presentación. La certificación la realiza la institución a solicitud personal del librador.

Cheque de Caja.- Se trata de documentos librados por la institución a su propio cargo y se usan generalmente para cubrir pagos de la propia institución, que por su naturaleza no conviene que se realicen en efectivo. Por tanto, no son negociables y sólo pueden endosarse para su control en la institución librada.

Cheques de Ventanilla.- Son cheques que la institución facilita a sus cuenta-habientes, a fin de que puedan librarlos contra su propia cuenta, en caso de que no traiga consigo su chequera y necesite disponer de fondos en ese momento.

Pago de Cheques Oficiales.- Este servicio consiste en el pago de todo tipo de cheques expedidos por dependencias gubernamentales, tales como: cheques de tesorería, de universidad, etc., sin cobrar comisión.

CREDITOS BANCARIOS

Prestamos Personales.- Este servicio consiste en que el banco presta dinero, a un plazo determinado, a personas físicas que poseen recursos medios o modestos, los cuales tengan que cubrir gastos de diversa naturaleza que impliquen una necesidad legítima y no suntuaria, tales como atención médica, compostura de inmuebles, tes. Este crédito no será otorgado para cubrir adeudos y las amortizaciones serán mensuales, para lo cual el deudor abrirá una cuenta de ahorros.

Prestamos Prendarios.- Este tipo de crédito se otorga sobre garantías reales, las cuales pueden ser títulos, valores o bienes muebles en general. En ningún caso el importe del préstamo será superior al 70% del valor de la garantía. Los bienes muebles que constituyan la garantía deben depositarse en almacenes de depósito.

Prestamos Refaccionarios.- Por medio de un contrato, la institución presta dinero a plazo determinado, ya sea a personas físicas o morales, las cuales invertirán el importe del crédito, en la adquisición de bienes materiales que incrementen el activo fijo de la empresa. Queda garantizado el crédito por los bienes raíces, así como por el mobiliario y equipo de la empresa, cuyo crédito ha sido destinado al fomento de la producción.

Prestamos Quirografarios.- Mediante estas operaciones, se otorgan créditos a personas físicas o morales que se dediquen a actividades comerciales e industriales. Normalmente se destinan a incrementar temporalmente el capital de trabajo o a resolver y a cubrir necesidades eventuales de tesorería (impuestos), a plazos cortos.

Prestamos Hipotecarios.- Este servicio consiste en otorgar créditos a la clientela para compra de casa-habitación. Queda garantizado el crédito con la hipoteca de la casa o terreno.

Préstamo de Habilitación o Avío.- Son créditos que el banco otorga a personas físicas o morales las cuales se obligan, mediante un contrato, a invertir el importe del préstamo en la adquisición de materias primas y materiales, en el pago de jornales y salarios, así como en gastos directos indispensable para la operación de la empresa.

Tarjetas de Crédito.- Este servicio consiste en la afiliación de negocios de diferentes ramos, para atención de los tarjeta-habientes, quienes, al identificarse por medio de la tarjeta expedida puede comprar artículos o servicios firmando un pagaré en lugar de pagar en efectivo.

Descuentos.- La institución otorga un crédito a nuestros clientes por medio de la adquisición de documentos con cargo a tercera; personas (girados o suscriptores) y efectúa el pago anticipado del valor de éstos. Los documentos con los cuales se efectúa el descuento provienen principalmente de operaciones mercantiles, las cuales pueden estar representadas por letras de cambio o pagarés no vencidos.

Prestamos para la Adquisición de Bienes de Consumo Duradero.- Estos créditos se otorgan únicamente a personas físicas y se destinan a la adquisición de bienes de consumo duradero, ya sea de línea blanca (refrigeradores, estufas, lavadoras, tes.) o bien de línea negra (radios, televisores, artículos eléctricos, tes.), así como vehículos de motor e instrumentos profesionales.

Los bienes deberán ser adquiridos en empresas productoras o dedicadas a la venta de estas mercancías.

Créditos Comerciales.- El banco contrae el compromiso de garantizarle al beneficiario de una transacción comercial (vendedor), el pago correspondiente a embarques o entrega de mercancía por parte del comprador (solicitante del crédito), siempre y cuando los documentos se apeguen estrictamente a las condiciones estipuladas y dentro de la vigencia del crédito.

SERVICIOS NACIONALES E INTERNACIONALES

Remesas en Camino Sobre el País.- Son documentos girados contra instituciones bancarias del interior de la República, los cuales se reciben por parte del cuenta-habiente, para abono en cuenta. Consiste en la entrega, mediante endoso, del título para hacerlo efectivo con la institución librada.

Remesas en Camino Sobre el Extranjero.- Son documentos girados contra instituciones bancarias del extranjero y se reciben para realizar un abono en cuenta o pago en efectivo, esto puede ser en cualquier clase de moneda.

Cobranzas del Interior.- Por medio de este servicio, los clientes pueden gestionar el cobro o aceptación de su cartera, pagadera en la plaza o fuera de la plaza, representado por: letra de cambio, pagarés, cheques y cobranzas.

Cobranzas del Extranjero.- El departamento de cobranzas del extranjero, sirve de intermediario entre el banco del extranjero y el banco del interior de la República, para cobrar o pagar a personas físicas o morales, que encomiendan a la institución documentos provenientes de operaciones de importación para tramitar su aceptación o cobro.

Ordenes de Pago.- Consiste en tramitar pagos fuera de la plaza donde se origina la orden, por conducto de nuestros corresponsales en el país o en el extranjero, de acuerdo con las instrucciones del solicitante.

Compra Venta de Giros Bancarios Internacionales y Nacionales.- Consiste en la expedición de un documento que ampare determinada cantidad de dinero para ser pagado a un beneficiario fuera de la plaza donde se originó la operación.

Los giros bancarios pueden ser expedidos en moneda nacional o extranjera.

Compra-Venta de Moneda Extranjera y Oro.- Consiste en cambiar tanto los billetes y moneda de otros países, así como el oro, a moneda nacional y viceversa, a los precios que fije el mercado.

Venta de Cheques de Viajero.- Consiste en la venta de cheques de diferentes denominaciones, emitidos por diferentes instituciones del extranjero y en su moneda extranjera. Dichos cheques son de aceptación internacional y equivalen a dinero en efectivo para el portador, mediante la comprobación de la firma de quien lo expide.

SERVICIOS RELACIONADOS CON VALORES

Compra-Venta de Valores.- Por conducto de la institución, se realiza la compra-venta de cualquier tipo de títulos que se cotizan en el mercado de valores y, por medio de esta operación, la institución actúa como comisionista, procurando obtener los mejores precios del mercado.

Futuros.- Es un contrato mediante el cual una persona física o moral se compromete a comprar o vender una divisa extranjera a un plazo determinado, pagando al comprador el importe correspondiente al tipo de cambio del día en que se celebró el contrato. Este servicio sólo se otorga en casos muy especiales.

SERVICIOS RELACIONADOS CON FIDUCIARIO

Avalúos.- Por medio de este servicio se les da a conocer a la clientela el justo precio de compra venta, de bienes muebles e inmuebles, ya que se utilizan los servicios de valuadores legalmente autorizados y de reconocida solvencia moral.

Compra-Venta de Inmuebles.- En este servicio, la institución sirve como intermediario en la compra y venta de inmuebles, ubicados en la República cobrando un pequeño porcentaje sobre las operaciones efectuadas.

Fideicomiso.- Son operaciones por medio de las cuales el cliente (fideicomitente) entrega determinados bienes o derechos a la institución fiduciaria, para que ésta los destine a conseguir un fin lícito y determinado y canalice los beneficios resultantes en favor de los beneficiarios (fideicomisarios) que el mismo cliente designe.

Mandatos.- Es un contrato por medio del cual, el cliente (mandante) encarga a la institución (mandatario), la ejecución de determinados actos lícitos, tales como invertir, administrar, etc.

OTROS SERVICIOS

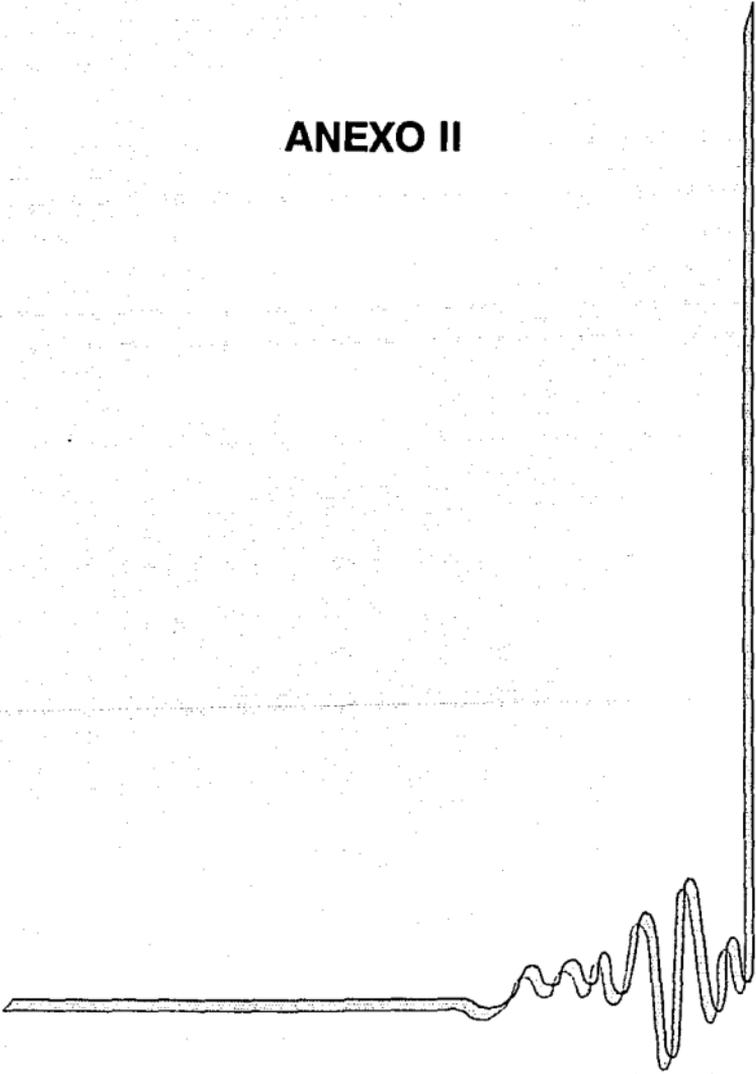
Pago de Servicios con Cargo a la Cuenta de Cheques.- La institución se encarga, por medio de un contrato con el cliente, que tiene una cuenta de cheques de pagar diversos servicios por cuenta del mismo, tales como : impuesto predial, luz, teléfono, gas, suscripciones a revistas y periódicos, póliza de seguro, hipotecas, etc.

Alquiler de Cajas de Seguridad.- Por medio de este servicio, proporciona un medio seguro de conservar y guardar toda clase de valores, tales como : alhajas, escrituras, documentos confidenciales, etc.

Se establece este servicio por medio de un contrato de arrendamiento entre la institución y el cliente, y el pago de una renta anual.

Además de mencionar los servicios que ofrecen, es importante destacar en cuales se está presentando problemas (inmovilización de capitales) : cuenta de cheques, cheque certificado, pago de cheques oficiales, tarjeta de crédito o débito, descuentos, cartas de crédito para viajeros, remesas en camino sobre el país y el extranjero, cobranzas del interior y extranjero, órdenes de pago, compra venta de giros bancarios internacionales y nacionales, cheques de viajero, fideicomiso, pago de servicios con cargo a cuenta de cheques.

ANEXO II



ANEXO II

DESCRIPCION DE LOS EQUIPOS DE LA RED

UNISYS 2200/400

Los sistemas 2200/400 consisten de 3 o más gabinetes asociados a sus periféricos. La versión de los sistemas se define por el número de procesadores de instrucciones con que se cuentan.

2200/401	1 Procesador
2200/402	2 Procesador
2200/403	3 Procesador
2200/404	4 Procesador
2200/405	5 Procesador
2200/406	6 Procesador

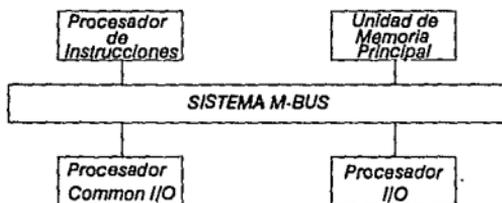
La mínima configuración del sistema es :

- 3 Gabinetes centrales
- 1 Procesador de instrucciones
- 1 Unidad de memoria central
(4 Megawords / 64 Megabytes)
- 1 Procesador de Entrada/Salida
- 1 Consola (PC)
- Periféricos Asociados.

La máxima configuración del sistema es :

- 7 Gabinetes centrales
- 6 Procesadores de instrucciones
- 4 Unidades de memoria central
(16 Megawords/64 Megabytes)
- 10 Procesadores de Entrada/Salida
- 2 Consolas (PC)
- Periféricos Asociados

La arquitectura del bus hace al sistema flexible, ya que el bus fue diseñado para soportar conexiones con los procesadores, unidades de almacenamiento y procesadores de entrada/salida que se necesitan.



Entre más procesadores de instrucciones tenga el sistema, más tareas se pueden atender al mismo tiempo.

Algunas de las principales ventajas del sistema son las siguientes :

- Crecimiento modular de procesadores de instrucciones
- Memoria compartida
- Sistema integrado de archivos
- Dispositivos de entrada/salida compartidos
- Gran potencial de crecimiento
- Recuperación automática en caso de corte de la energía eléctrica.

Unidades de Entrada/salida

La arquitectura de Entrada/Salida del sistema 2200/400 consiste de las siguientes partes:

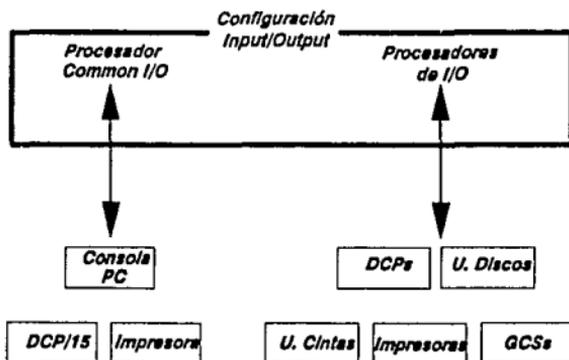
- Procesadores de Entrada/Salida (IOPs)
- Block Multiplexer Channels (BMCs) y Word Channels (WDCs)

- Procesador común de Entrada/Salida (CIOP)

Los procesadores de Entrada/Salida son el corazón de la arquitectura. En un sistema expandido puede tener hasta 10 procesadores, con esta arquitectura puede soportar hasta 40 canales.

Los Block Multiplexer Channels y los Word Channels son controlados por los IOPs. Estos soportan dispositivos de alta velocidad como son discos, cintas, procesadores de comunicaciones alternos y los subsistemas generales de comunicación.

El procesador común de Entrada/Salida es un canal de baja velocidad y puede utilizarse para conectar la consola, impresoras lentas y DCP/s5



La 2200/400 usa las ventajas de los DCPs para conectarse a varios tipos de terminales, workstations remotas, PCs, controladores clusters, a múltiples host Unisys, a hosts IBM, procesadores Front-End y a redes públicas de datos.

Los DCPs disponibles son DCP/15, DCP/20, DCP/40 y DCP/50.

Software del Sistema

El software del sistema consiste del EXEC (Executive), cuya función principal es la de supervisar y mantener el entorno de operación con máxima eficiencia y nos brinda facilidades para :

- Estructuras de programa
- Manejo de memoria principal y almacenamiento secundario.
- Asignación de dispositivos.
- Monitoreo del sistema por los usuarios
- Monitoreo de las actividades y mensajes
- Capacidad para comunicar a los usuarios con el sistema operativo.

Operación y Administración del Software

Una ayuda para la operación es una herramienta que corre en la consola que ayuda a controlar el sistema, su operación y da un diagnóstico del estado que guarda. En forma general se tienen 4 categorías de operaciones que se realizan en la consola :

- Operación del sistema
- Control del sistema
- Utilerías de la consola
- Diagnóstico por monitoreo

Estas categorías son presentadas al operador en forma separada (diferentes pantallas). El operador selecciona una y las otras continúan en background.

Comúnmente sólo la sesión de operación del sistema es necesaria.

Operación del Sistema

Consiste en mensajes enviados por el sistema a la consola y el operador los contesta desde el teclado.

La consola funciona bajo 3 niveles de interacción con el operador :

- Modo de Atención : En todo el tiempo el operador es requerido, este es el modo básico de operación del sistema.
- Modo Casual : El sistema corre solo, y cuando requiere una intervención del operador, el sistema activa una alarma.

- **Modo sin Atención :** El sistema corre completamente solo sin atención.

Estos 3 modos funcionan de acuerdo a las necesidades, por ejemplo, el sistema corre en modo de atención cuando se prende en la mañana, corre durante el día en modo casual y muchas veces durante la noche corre sin atención.

Control del Sistema.

Es manejado por el System Control Facility (SCF) y entre sus funciones se destacan :

- Inicialización del equipo central
- Diagnóstico del hardware.

Utilerías de la Consola

Son numerosas las utilerías que corren en la consola, el operador las usa para controlar diferentes características de operación como :

- Habilitar/Deshabilitar el diagnosticador de interfaces
- Habilitar/Deshabilitar impresoras
- Habilitar/Deshabilitar usuarios

Diagnóstico por Monitoreo

Si en el equipo central ocurre una falla, lo reporta a la consola en forma automática, dando una descripción de la situación. El programa de diagnóstico corre en forma independiente de las tareas de la consola.

Ambiente para Usuarios Finales

El sistema 2200/400 ofrece los siguientes 4 ambientes para los usuarios finales :

- MAPPER SYSTEM que es un sistema de cuarta generación.
- Link Office System (OFIS) para automatización de oficinas

- Computadoras Personales (PCs)
- Unix (SX 1100)

El sistema MAPPER funciona como un :

- Lenguaje de cuarta generación
- Generador de aplicaciones
- Procesador de transacciones
- Manejo de base de datos
- Report writer
- Procesador de palabras
- Sistema de planeación y control
- Sistema de soporte de decisiones

El sistema de automatización de oficinas (OFIS) ofrece :

- Transferencia de información por medio de un correo electrónico y archivos compartidos
- Procesador de palabras que permite editar, formatear y hacer merge con los archivos.
- Formateador de documentos

Las computadoras personales se acoplan muy bien al OFIS, ya que se pueden usar como máquinas de escribir, procesador de palabras, PC y como ventana al correo electrónico.

Computadoras Personales

Unisys tiene el siguiente software para comunicarse con el sistema 2200/400 :

- Terminal Emulation Package (STEP)
- PC/On line
- Information Services PC (IS-PC)

Terminal Emulation Package

Transforma la PC en una terminal con capacidad de correr 8 sesiones al mismo tiempo. El paquete consiste en :

- Tarjeta de expansión con puerto serial

- Software para emular 7 diferentes tipos de terminales.

PC/On Line

Hace las mismas funciones que el STEP, pero existen las siguientes mejoras :

On Line Disk

Que extiende el poder de la PC al usar el sistema 2200/400 para acceder la memoria secundaria y las impresoras.

On Line Extract

Provee puente entre el sistema MAPPER y las aplicaciones en la PC.

On Line Transfer

Provee facilidades para transferencia de archivos ASCII en forma síncrona.

Information Services PC (IS-PC)

Integra al usuario de la PC al ambiente Distributed System Services (DSS).

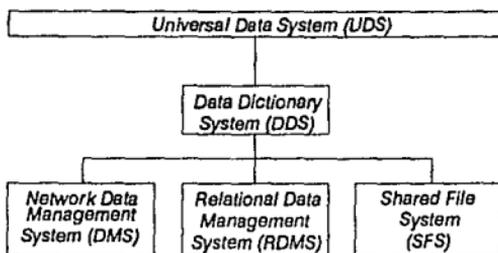
Manejador de Base de Datos

El sistema 2200/400 maneja diferentes organizaciones para mantener sus sistemas de datos :

- Universal Data System (UDS)
- Processor Common Input/Output System (PCIOS)
- Information Management System (IMS 1100)

Universal Data System (UDS)

Dentro del UDS se tienen 3 manejadores independientes en una arquitectura :



Todos los archivos, pueden ser accedados vía DMS, RDMS o SFS, tratados por el UDS como una sola base de datos.

El UDS tiene los siguientes componentes :

- Un módulo de control (UDS control)
- Una utilería de Backup y Recovery (Integrated Recovery Utility IRU)
- Una utilería para definición de la base (Data Dictionary System DDS)
- Los 3 manejadores DMS, RDMS y SFS.

Processor Common Input/Output System (PCIOS)

En PCIOS se pueden tener archivos compatibles para utilizarse entre los procesadores, utilerías y un Query, además, una cosa importante, es que se pueden compartir archivos en forma concurrente. El Query (Query Lenguaje Processor QLP) que contiene una serie de comandos y facilidades para hacer reportes.

Information Management System (IMS 1100)

IMS es un sistema transaccional con un manejador de archivos. Este manejador tiene una serie de transacciones que se pueden ejecutar desde un programa o en línea.

Comunicaciones

Unisys, tiene el software y hardware necesario para comunicarse con terminales, otras computadoras, redes de datos y algunas otras redes públicas.

Se tienen 3 componentes principales de software:

- Communications Management System (CMS 1100) que es un estandar de comunicaciones.
- Software Telcon. El cual opera en un DCP (Distributed Communications Services).
- Distributed System Services. Provee facilidades para usuarios finales, como transferencia de archivos, comunicación de programa a programa, etc.

Unisys emplea una arquitectura distribuida de comunicaciones (DCA), esta se basa en los conceptos y estructuras de la OSI.

El sistema es flexible en su configuración, es decir, su configuración puede expandirse en cualquier dirección. Diferentes productos pueden ser conectados vía DCA:

- Computadoras Personales
- Múltiples tipos de terminales tontas
- Clusters
- Máquinas Unisys series 1100 y 2200

También puede soportar comunicación con productos de diferente marca:

- Varios tipos de terminales vía BSC, SNA y TTY.
- Computadoras IBM
- Redes SNA
- Redes Públicas (Public Data Network PDN)

CMS 1100 es un estándar de comunicaciones que contiene diferentes dispositivos:

DCP/Telcon System

Los DCPs tienen las siguientes características :

- Conexiones con terminales remotas, computadoras Unisys, computadoras IBM, redes públicas de datos y otros DCPs.
- Conexiones con dispositivos periféricos como terminales, impresoras, discos, diskette y cintas magnéticas.
- Maneja gran variedad de configuraciones asíncronas, síncronas y diferentes anchos de banda.
- Soporta transacciones, tiempo compartido, entrada remota de trabajos y procesos distribuidos de aplicaciones simultáneas.

El software de Telcon corre sobre los procesadores distribuidos de comunicaciones y éste puede ser estructurado para cualquier requerimiento. Por su parte, Telcon contiene :

- Sistema Operativo (DCP/OS)
- Software de interface para comunicarse con los manejadores.
- Software de la red para mantenimiento, mandar mensajes y funciones de control.
- Puede configurarse para soportar los siguientes ambientes :
 - Procesadores Front-End (FEPs), conectados a un sistema de Host.
 - Concentradores Remotos (RCs)

Ambiente de Redes

La 2200/400 puede ser usada en una variedad de ambientes de comunicaciones, estos ambientes incluyen :

- Unisys a Unisys
- Unisys a otras marcas de computadoras.

SISTEMA 38 DE IBM

La arquitectura del Sistema 38 de IBM se basa en tres funciones clave : el Sistema Operativo (CPF), manejo de memoria a un solo nivel y una base de datos relacional integrada.

Sistema Operativo (CPF).

El CPF proporciona una interfaz de alto nivel para todas las funciones, configuraciones del sistema y tipos de aplicaciones, esto asegura la compatibilidad de aplicaciones de software en toda la gama de modelos del Sistema 38, y la posibilidad de añadir nuevas funciones, dispositivos adicionales y mejoras del rendimiento a sistemas existentes, sin afectar los programas de aplicación.

Manejo de Memoria a un Solo Nivel.

Los programadores no están limitados por tamaños de programas específicos, áreas de tareas o ubicación de datos en las unidades de disco, ya que el Sistema 38 trata la memoria principal y la auxiliar como una sola unidad. El resultado es un manejo de memoria más eficaz, independiente de los programas y de cambios en la capacidad de los discos, y reducción del trabajo de diseño y planificación de aplicaciones.

Base de Datos Relacional Integrada.

Tiene una base de datos relacional integrada como parte del software del sistema (CPF). Esta integración a nivel de diseño proporciona un mayor rendimiento, seguridad, integridad y facilidad de uso de la base de datos.

El Sistema 38 puede tener una memoria principal máxima de 32 MB y permite la conexión de hasta 256 estaciones de trabajo locales.

Almacenamiento en Disco

Pueden conectarse hasta 14 GB de almacenamiento adicional utilizando el subsistema de almacenamiento de acceso directo IBM 9335 y los dispositivos de almacenamiento de acceso directo IBM 9332.

Posibilidades de Conexión.

Se puede utilizar como sistema departamental dentro de una gran red central o como procesador central en una red de sistemas más pequeños. El adaptador de líneas de comunicaciones ofrece hasta 12 líneas para transmisión de datos a velocidades de hasta 57,600 bps. Estas líneas pueden utilizarse para comunicarse en los protocolos SNA/SDLC y BSC en redes conmutadas, no conmutadas o con la red Telepac X.25.

El dispositivo de conexión a X.25 admite hasta 64 circuitos virtuales a velocidades de hasta 64 kbps y puede utilizarse también para conexiones locales con otros sistemas que soporten la conexión X.25 a alta velocidad. En este caso, el Sistema 38 actúa como un puerto de una red X.25.

El Sistema 38, con el adaptador digital (DDSA), también admite comunicaciones remotas a velocidades de hasta 56,000 bps en redes digitales.

Utilizando los controladores de estaciones de trabajo, el sistema 38 puede admitir hasta 256 estaciones de trabajo, estas pueden estar a una distancia máxima de 1500 m. de la unidad central, permitiendo conectar hasta siete dispositivos en un solo cable.

El sistema 38 proporciona herramientas para facilitar el manejo y disponibilidad de su red de comunicaciones. Esto es posible por que cuenta con :

- Un registrador de tráfico de comunicaciones y uno de errores de datos a través del Programa de Análisis Estadístico de la Red de Comunicaciones (CSNAP), esta información se puede usar como ayuda para identificar fallas en la línea o en dispositivos, así como para ajustar el rendimiento.
- Una facilidad llamada COMMTRAP, proporciona un método para aislar problemas de comunicaciones o de la información de los usuarios a velocidades de línea de hasta 9,600 bps sin la necesidad de un seguimiento adicional del hardware.

El Soporte para comunicaciones incluye una utilería llamada Control Program Facility (CPF). Utilizando este soporte, los programas de aplicación del Sistema 38 pueden comunicarse como un procesador central con un amplio rango de sistemas y terminales bajo BSC y SNA.

Unidad de Proceso.

Las funciones ejecutadas bajo la interfaz de la máquina de alto nivel incluye:

- Búsqueda de programas o archivos.
- Asignación de memoria.
- Manejo de colas.

El manejador de memoria de un solo nivel maneja la memoria principal y el almacenamiento auxiliar como un solo recurso.

Se pueden conectar hasta 128 estaciones de despliegue y/o impresoras directamente al sistema

Proporciona la capacidad de comunicación con los sistemas de despliegue de información IBM vía SNA/SDLC.

Soporta de 1 a 4 enlaces para comunicaciones de datos por controlador.

Se pueden conectar las siguientes estaciones de despliegue :

- IBM 5251
- IBM 5291 Modelo 1
- IBM 5292
- IBM 3262

Se pueden conectar las siguientes impresoras :

- IBM 3262
- IBM 5219
- IBM 5224
- IBM 5225
- IBM 5256
- IBM 3203-5

SNA (System Netware Architecture)

Es un esquema propuesto por IBM, orientado al procesamiento distribuido y a la administración de las comunicaciones, es un conjunto de estándares de interconexión de productos de hardware y software. SNA tiene como objetivo proveer :

- Un mecanismo de distribución de funciones, que mueva algunas tareas de la computadora central, a los periféricos del sistema y equipos remotos.
- Independencia de conexión, de tal forma que diferentes tipos de equipos puedan conectarse al mismo enlace, usando un protocolo común, SDLC (Synchronous Data Link Control).
- Independencia del dispositivo, a efecto de que las aplicaciones sean escritas sin tener en cuenta las características específicas del dispositivo a ser usado.
- Flexibilidad de configuración, para que ésta pueda ser cambiada con facilidad.

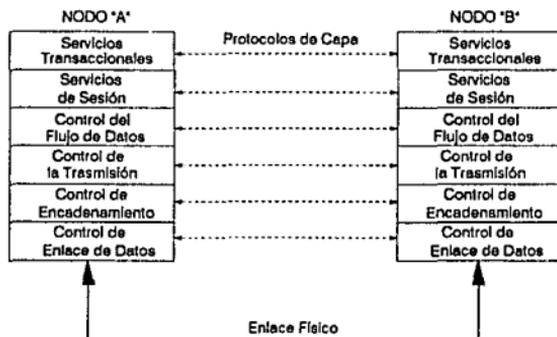
La topología básica de una red SNA consta de dos niveles, un primer nivel que llamamos dominio, consiste en nodos tributarios (terminales, clusters) de un nodo principal (host processor) al que están conectados por medio de sistemas diversos de comunicación y a través de nodos auxiliares.

En SNA se distinguen cuatro tipos de datos :

- Datos de aplicación, los cuales pueden ser incompatibles con la forma de operar del usuario final al cual se destinan los mismos, por ejemplo, datos que son resultado de la capa de aplicación, o de un usuario final.
- Comandos SNA, usados para activar, controlar y desactivar la red, también tienen aplicación en el establecimiento, control y terminación de sesiones entre usuarios finales.
- Datos de respuesta, que indican si la información recibida es aceptada o no, y en caso negativo cuál es la causa del rechazo.
- Datos de encabezado, los cuales existen siempre agregados a los tres tipos anteriores. Consisten en indicadores de control e información para el correcto enrutamiento de los mensajes.

SNA tiene 6 capas diferentes, las cuales no incluyen a la capa física por su simplicidad y porque ya está estandarizada a través de los diferentes organismos internacionales, esta capa se encarga de establecer las características físicas de la conexión entre 2 nodos adyacentes y usa un protocolo propio para trasportar las señales del origen al destino.

Para entender la operación de SNA, es necesario conocer el esquema en capas :



CAPAS DEL SNA

Capa de Control de Enlace de Datos (DLC: Data Link Control), establece las reglas que gobiernan las comunicaciones en una línea que conecta dos nodos adyacentes y a través de la cual se transmitirá el mensaje. Especifica un protocolo de capa llamado SDLC o un protocolo para el canal de E/S de la computadora. Existe un componente DLC por cada línea de comunicaciones del nodo.

Capa de Control de Encadenamiento (PC : Path Control), ejecuta la función de ruteo dentro de los nodos, asigna a los mensajes un camino primario o alternativo cuando existen condiciones que así lo determinen. Dentro de esta capa existen dos funciones que determinan el siguiente paso a dar, a estas rutas se les llama "ruta explícita" y "ruta virtual". En cada nodo, el PC selecciona el próximo nodo al cual se le enviarán los datos y el enlace que se utilizará para tal efecto, usando direcciones (NA: Netware Address) y una tabla de ruteo (RT: Routing Table). En algunos casos (cuando se llega a un nodo periférico), el PC transforma la NA en una dirección local y para ello usa una tabla suplementaria de ruteo (SRT: Supplemental Routing Table). Además, encuadra los datos dentro de un tamaño constante, de acuerdo a la capacidad del protocolo que se usa en el siguiente tramo del camino elegido, ya sea segmentando mensajes muy largos, o combinando bloques que se dirigen al mismo destino inmediato, existe solamente una capa de este tipo (PC) por nodo.

Capa de Control de Transmisión (TC: Transmission Control), es responsable de mover los mensajes desde el nodo de origen hasta el nodo destino, aún a través de nodos intermediarios, administra la tasa de transferencia de mensajes, previniendo sobre la carga y mejorando la utilización de la línea, administra también el correcto secuenciamiento de mensajes de datos, dentro de una sección de comunicaciones, rutea los mensajes hacia el usuario final o hacia otras capas de control (DFC y TC), según sea la naturaleza de los mismos.

Como una medida de seguridad, el TC puede encriptar o desencriptar los datos, esto es conocido como "Criptografía a nivel de sesión".

Capa de Control del Flujo de Datos (DFC: Data Fluency Control), realiza la mayoría de las funciones de mantenimiento de la integridad de los datos, que se transmiten en una sesión de comunicaciones, además de realizar las siguientes tareas :

- Modos de Envío/Recepción
- Encadenamiento (Chaining)
- Opciones de Respuesta.

Modos de Envío/Recepción. La transmisión de datos a través de una red SNA puede ser de 3 maneras diferentes :

- Full-Duplex. El flujo es bidireccional entre las entidades involucradas en la sesión.
- Half-Duplex Flip-Flop. El sentido de transmisión se alterna entre las partes, donde una de ellas dirige el tráfico (este modo es apropiado para situaciones de consulta/respuesta).

- **Half-Duplex Contention.** Cualquiera de las partes puede comenzar el envío de datos a la otra.

Encadenamiento (Chaining). Si existen mensajes que van a ser enviados a la misma dirección se agrupan lógicamente en una unidad mayor llamada cadena, en donde si en uno de sus eslabones se detecta un error, causa que toda la cadena se ignore y se invoque el procedimiento de recuperación.

Los brackets, consisten en secuencias relacionadas de cadenas de mensajes que fluyen en ambas direcciones, entre un par de entidades lógicas en sesión. Esto permite que aquellas aplicaciones que procesan secuencias de transacciones en una sesión dada, mantengan los datos relacionados a otras transacciones.

Opciones de respuesta. Se permiten distintos tipos de respuestas de reconocimiento a un mensaje enviado.

Existe un elemento DFC, por cada usuario final en sesión.

Los Servicios a las Sesiones de la Red, se dividen por la función que realizan :

- **Servicios de Configuración.** Ayudan a controlar los recursos asociados con la configuración física de la red, incluyen la activación y desactivación de enlaces entre nodos y permite al operador de la red alterar la configuración de la misma.
- **Servicios al Operador de la Red.** Dan facilidad de comunicación entre los puntos de control y los operadores de la red, proveen los medios para ejecutar comandos para arrancar y detener la red, activando y desactivando los recursos y llevando bitácoras de errores en los nodos.
- **Servicios de Sesión.** Ayudan a activar y desactivar sesiones cuando así se solicita. Una de sus principales funciones es convertir los "nombres" de los elementos que inician una sesión en "direcciones de la red".
- **Servicios de Monitoreo y Mantenimiento.** Permiten que un punto de control ejecute varias pruebas para determinar si un enlace o un nodo ha fallado y por qué razón. Además, ayuda a llevar estadísticas de errores ocurridos en los nodos.

Servicios a los Usuarios Finales (Transaccionales). Estos servicios se dividen en dos categorías : de presentación y de aplicación.

Servicios de Presentación (PS: Presentation Services). Definen el puerto de acceso a la red SNA por un usuario final, en términos de :

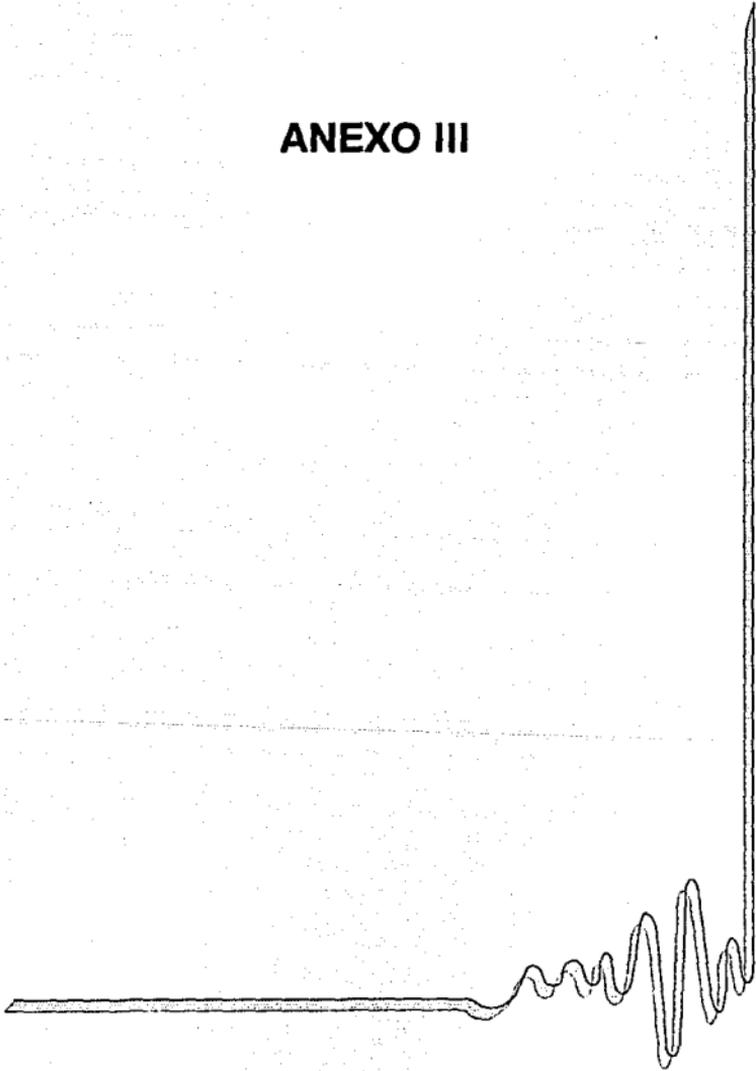
- Requerimientos de traducción de códigos y comandos.
- Formato de pantallas, atributos de video, etc.
- Compactación de datos.

Se encarga de que los mensajes sean compatibles con las características del usuario final de destino.

Las terminales tontas, tendrán muy limitados servicios de presentación, esta función esta relegada a la inteligencia de la cual depende la terminal.

Servicios de Aplicación a Aplicación. Estos son servicios definidos para aquellas sesiones que vinculan dos sistemas de procesamiento transaccional. En otros casos, permiten que un programa de aplicación obtenga acceso a una base de datos, sin saber dónde se encuentra ésta en la red, y otro servicio puede ser la forma para que dos o más programas de aplicación sincronicen sus actividades (por ejemplo, la actualización simultánea de registros relacionados en una base de datos distribuida).

ANEXO III



ANEXO 3

TIPOS DE MUESTREO

MUESTREO DE CRITERIO.

Este muestreo se fundamenta en la capacidad y experiencia profesional del auditor, para lo cual es necesario contar con:

- 1) Educación teórica suficientemente amplia en el campo en que esté practicando la evaluación, para que pueda seleccionar sus muestras, de tal forma que se incluyan todas las características de la población.
- 2) Experiencia práctica suficiente para poder comparar los resultados de una muestra con los resultados observados a través de su experiencia.
- 3) Juicio equilibrado y maduro, que le permita estimar objetivamente todos los elementos que van a influir en su operación.

El muestreo de criterio, es el más utilizado en la auditoría y no por ser mejor sino porque es el más sencillo de aplicar.

Para este muestreo, la selección de muestras se puede llevar a cabo de la siguiente forma:

- a) Selección a juicio del auditor.
- b) Selección por intervalos.
- c) Selección por bloques o conglomerados.
- d) Selección por números aleatorios.

Selección a juicio del auditor. Este método es aquel que se aplica a entero juicio del auditor. No lleva ningún patrón, norma ni procedimiento estadístico.

Selección por intervalos. En este método la selección más importante del auditor está representada al definir el tamaño del intervalo.

La forma de obtener el intervalo es:

$$i = N/n$$

donde: i = intervalo
 N = Total de la población
 n = Número a seleccionar

En este método se requiere que la primera muestra sea seleccionada al azar y las restantes sean extraídas utilizando el intervalo de muestreo.

Selección por bloques o conglomerados. Consiste en seleccionar, sobre la base de criterio, una parte de la población y revisarla al cien por ciento.

Selección por números aleatorios. Este método de selección consiste en someter a una población determinada por números aleatorios.

MUESTREO ESTADISTICO.

Es aquel en que la determinación del tamaño de la muestra, la selección de las partidas que la integran y la evaluación de los resultados, se hace por métodos matemáticos basados en el cálculo de probabilidades.

Para que este muestreo estadístico sea aplicable en auditoría y se obtengan resultados confiables, se requiere lo siguiente:

- 1) Masividad en los datos a examinar, ya que las conclusiones se basan en la teoría de probabilidad.
- 2) Homogeneidad de las partidas a examinar, se necesita para garantizar que la muestra sea representativa del universo.
- 3) Que la selección de la muestra sea aleatoria.

El método consiste:

- 1) **Diseño de la muestra.** Determinar el tamaño apropiado de la muestra seleccionada para extraer conclusiones sobre la información.
- 2) **Selección de la muestra.** Consiste en la identificación de eventos.

- 3) **Evaluación de la muestra.** Es la formación de conclusiones acerca de la información que proporciona la muestra.

Cabe aclarar que estos criterios no substituyen al criterio profesional del auditor.

Conceptos básicos del muestreo estadístico

Nivel de confianza.- Puede considerarse como el grado en que es justificado estimar que una muestra aleatoria indica el verdadero valor del universo del cual se extrajo la muestra. De otra forma, es la probabilidad de que el valor de la muestra, de las características en estudio de una población y esta no difiera del verdadero valor del universo en más de una cantidad establecida (precisión). El nivel de confianza generalmente se expresa como porcentaje. De esta forma si se habla de un nivel de confianza de 98% se quiere decir que hay 98 posibilidades de entre 100 de que los resultados de la muestra representen las condiciones verdaderas del universo frente a dos posibilidades de que no las representen.

Precisión.- Es la amplitud dentro de la cual debe encontrarse la respuesta verdadera concerniente a las características de la población que se estudia con un determinado nivel de confianza. Dicho de otra forma, es el grado de exactitud del supuesto de que el número de errores de la muestra se aplica proporcionalmente a la parte no muestreada de la población. De tal suerte, si con base en una prueba se afirma que la tasa de error proyectada en un universo dado es 5% +/- 2%, se está diciendo que la tasa de error en la muestra examinada fue exactamente de 5%, en tanto que la precisión en la muestra era de +/-2%.

Esto es, la posible tasa de error del universo puede ser tan pequeña como el 3% o tan grande como el 7%.

Tasa de error esperada.- Es el porcentaje de error que el auditor se encontrará como resultado de una prueba, para estimar la tasa de error el auditor podrá guiarse por los resultados de una auditoría previa, por un estudio preliminar, o por una prueba piloto. El auditor debe ser realista al estimar la tasa de error esperada.

El método de muestreo estadístico se puede llevar a cabo por varias formas de muestreo, solo veremos el de atributos y el de variables.

MUESTREO DE ATRIBUTOS.

Esta modalidad de muestreo tiene como objetivo determinar los atributos o características cualitativas de una muestra de auditoría y precisar si el área sujeta a auditoría esta cumpliendo con los requisitos de control interno establecidos para la verificación de las muestras seleccionadas.

- 1) Con base en el juicio, criterio, capacidad técnica y conocimientos previos que se tengan de la población sujeta a examen, se deberá determinar el nivel de confianza (el más utilizado es 95%), precisión (tolerancia) y tasa de error.
- 2) Una vez que se tengan definidos los conceptos anteriores, el auditor deberá conocer el tamaño del universo o población seleccionada, posteriormente utilizando las tablas que se encuentran al final del anexo (cuadro A) se determinara el tamaño de la muestra.

En estas tablas se puede apreciar que el tamaño de la población varia de 50 a 500,000, la tasa de error no mayor de 2 tendrá niveles de confianza de 90% y 95%; para niveles de error no mayores de 3% se tendrá niveles de confianza de 90% y 95% y para niveles de error no mayores de 5% se tendrá también niveles de confianza de 90% y 95%.

Para entender un poco más el funcionamiento de estas tablas veremos el siguiente ejemplo:

Si tengo una población de 11000 y una tasa de error de 2.5% y un nivel de confianza de 95%.

La solución se obtiene como sigue :

Nos vamos al cuadro donde la tasa de error sea menor de 3 y tenga un nivel de confianza de 95%. Ahí buscamos el tamaño de la muestra, como para este caso fue exacta, el tamaño de la muestra es 176.

Para el caso de que el tamaño de la muestra no se encuentre en la tabla, es decir, si tuviéramos una población de 3,300 con una tasa de error de 1%, tenemos que obtener el valor menor y mayor inmediato, para este caso 3250 son 921 (menor) y para 3500 son 940 (mayor), se realiza lo siguiente :

$$921 + (3300-3250) * (940 - 921) / (3500 - 3250) = 924$$

De lo que concluimos que la muestra es de 924.

MUESTREO DE VARIABLES

El auditor emplea este método de muestreo cuando desea estimar el valor de una población compuesta de elementos que tienen características variables, las cuales pueden ser dólares, libras, días, meses, horas, etc.

Procedimiento

- 1) Determinación del tamaño de muestra, para este procedimiento es relativamente fácil cuando se utilizan las tablas (cuadro B) que se encuentran al final del anexo que han sido diseñados para utilizarse en este muestreo. Para usar este cuadro el auditor deberá tomar en consideración los siguientes datos:

El número aproximado de elementos en el grupo de datos que se va examinar (tamaño de la población).

- 2) El nivel de confianza.
- 3) El error de muestreo estipulado.
- 4) La razón de error de muestreo a desviación estándar.

Como ya se conocen los dos primeros conceptos definiremos los dos últimos.

Cálculo de la desviación estándar. Mientras mayor sea la variabilidad, mayor será el valor de la desviación estándar. Para obtenerla se procede de la siguiente manera: se calcula la diferencia entre cada elemento de la población y su media, se eleva al cuadrado cada una de estas diferencias, se suman los cuadrados, se divide luego la suma así obtenida entre el número total de los elementos y, finalmente, se extrae la raíz cuadrada de ese cociente.

Dado que el cálculo de la desviación estándar es tediosa y lleva mucho tiempo, el auditor prefiere utilizar una estimación.

Esta estimación para propósito de auditoría se puede obtener utilizando la amplitud de los valores de los elementos de la muestra preliminar y aplicando un factor estadístico de corrección.

Para determinar la desviación estándar estimada por el método de la amplitud promedio se sigue el siguiente procedimiento.

- 1) Utilizando números aleatorios, se seleccionarán alrededor de 50, este número dependerá del tamaño de los subgrupos que se escojan 6, 7 u 8 elementos, lo que significa que el grupo sea de 48 o 56 elementos.
- 2) Ordenar los elementos, es decir, los primeros 6 (7 u 8), se ordenarán por algún parámetro de la muestra y así los siguientes grupos.
- 3) Calcular la amplitud de los valores de cada grupo (la amplitud es la diferencia entre los elementos de valor más bajo y el de valor más alto).
- 4) Sumar las amplitudes de todos los grupos y dividirse esta suma entre el número de grupos, a fin de calcular la amplitud promedio de valores.
- 5) Calcular la desviación estándar estimada de la población dividiendo la amplitud promedio, obtenida según lo dicho en el punto 4, llamado factor d2.

Este factor es ampliamente utilizado en trabajos de control estadístico de calidad.

Tamaño de grupo	Factor d2
5	2.326
6	2.534
7	2.704
8	2.847
9	2.970
10	3.078
1(*)	

Cálculo de la razón de error de muestreo a desviación estándar.

Determinar el error de muestreo estipulado en términos del valor promedio. Como ya se dijo, cuando se muestrean variables el error de muestreo es la diferencia, frecuentemente expresada como un porcentaje, entre el valor promedio real de los elementos de la población bajo examen y el valor promedio de los elementos estimados con base a una muestra.

1(*) Fuente: Defense Contract Audit Manual

Ya con todos los elementos se utilizarán las tablas (cuadro B).

Ejemplo:

Si se tiene una muestra aproximada de 15,000 transacciones, con un nivel de confianza del 98%.

Por el método la estimación de la desviación estándar, realizaremos lo siguiente :

PASO 1.

Se tendrán 6 grupos de 8 elementos cada uno, es decir, se maneja una muestra preliminar de 48 elementos.

Grupo 1		Grupo 2	
No Transacción	Monto	No Transacción	Monto
80	1'200,000	578	3'720,500
11	7,820	1300	570,000
48	800,000	73	18,300
49	40,000	821	1'500,000
400	30'000,000	734	61,000
810	1'320,000	348	216,000
1200	10,000	58	341,200
638	117,380	1102	938,500
Menor	7,820		18,300
Mayor	30'000,000		3'720,500

Grupo 3		Grupo 4	
No Transacción	Monto	No Transacción	Monto
310	13'000,000	315	50,500
731	450,000	63	270,000
659	810,000	1308	415,000
890	110,000	491	1'800,000
870	80,000	330	33,100
77	4'000,000	237	173,900
38	500,000	823	300,000
399	814,000	621	2'500,000
Menor	80,000		33,100
Mayor	13'000,000		2'500,000

Grupo 5		Grupo 6	
No Transacción	Monto	No Transacción	Monto
257	130,000	809	14'000,000
600	100,000	546	800,000
725	511,000	373	1'300,000
912	18,000	120	2'700,000
949	45,000	711	10'000,000
791	197,000	405	1'600,000
68	19,000	90	3'400,000
24	330,000	14	8'500,000
Menor	18,000		800,000
Mayor	511,000		14'000,000

PASO 2

Grupo			
1	30'000,000 -	7,820 =	29'992,180
2	3'720,500 -	18,300 =	3'702,200
3	13'000,000 -	80,000 =	12'920,000
4	2'500,000 -	33,100 =	2'466,900
5	511,000 -	18,000 =	493,000
6	14'000,000 -	800,000 =	13'200,000
			62'774,280

$$62'774,280 / 6 = 10'462,380$$

$$\text{Factor } d2 = 2.847$$

$$10'462,380 / d2 = 3'674,878.82$$

Dado que la confiabilidad es 2

$$10'462,380 (2\%) = 209,247$$

$$\text{Error: } 209,247 / 3'674,878.82 = 5.7 \%$$

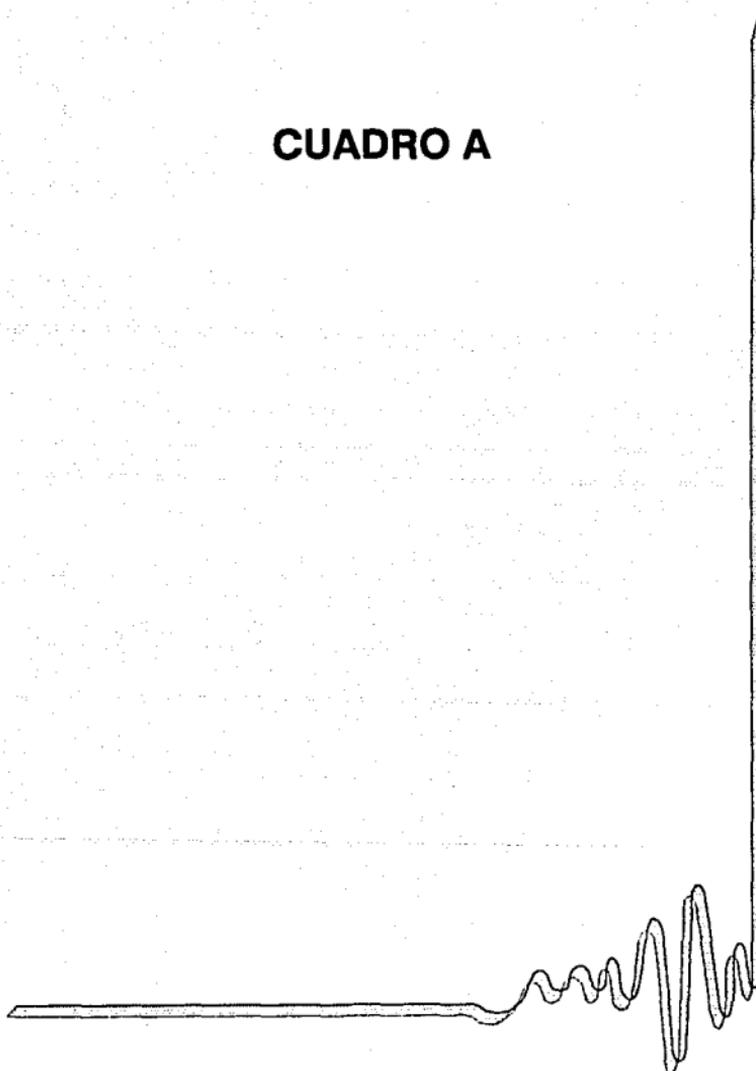
Redondeando 6%

Para utilizar la tabla tenemos 0.06

Sí nos vamos a las tablas del Cuadro B

Con una población de 15,000 y un nivel de confianza del 98% y con una razón de error de 0.06 tenemos una muestra de tamaño 1,367.

CUADRO A



Tamaños de la muestra para el muestreo de atributos.
Tasa de error esperada no mayor de 2%
Nivel de confianza de 90 %

Tamaño de la Población 1 (*)	Tamaño de muestra correspondiente a un porcentaje de precisión de más o menos :						
	0.50	0.75	1.00	1.25	1.50	1.75	2.00
50	48	47	45	43	41	38	36
100	95	90	84	77	70	63	57
150	140	129	116	104	91	80	70
200	182	165	145	125	108	92	79
250	223	197	169	143	121	102	8
300	262	227	191	159	132	109	91
350	300	255	210	172	140	115	96
400	336	280	228	183	148	120	99
450	371	304	243	193	154	125	102
500	404	326	257	202	160	128	104
550	436	347	270	209	165	131	106
600	467	366	281	216	169	134	108
650	497	384	292	222	172	136	110
700	526	401	301	228	176	138	111
750	554	417	310	233	179	140	112
800	580	432	318	238	182	142	113
850	606	447	326	242	184	143	114
900	631	460	333	246	186	145	115
950	656	473	340	250	188	146	116
1000	679	485	346	253	190	147	117
1100	724	507	357	259	194	149	118
1200	766	528	367	264	197	151	119
1300	806	546	376	269	199	152	120
1400	843	563	384	273	201	154	121
1500	878	578	391	276	203	155	121
1600	912	593	398	280	205	156	122
1700	943	606	404	282	207	157	123
1800	973	618	409	285	208	157	123
1900	1002	630	414	287	209	158	123
2000	1029	640	419	290	210	159	124
2250	1091	664	429	294	213	160	125
2500	1147	684	437	298	215	161	125
2750	1197	702	444	302	217	162	126
3000	1242	717	450	304	218	163	126
3250	1283	730	455	307	219	164	127
3500	1320	742	460	309	220	165	127
3750	1354	753	464	311	221	165	128
4000	1386	763	468	312	222	165	128

1(*) Fuente : Lockheed-Georgia Company, Grupo de Análisis Matemático

Tamaños de la muestra para el muestreo de atributos.
Tasa de error esperada no mayor de 2%
Nivel de confianza de 90 %

Tamaño de la Población	Tamaño de muestra correspondiente a un porcentaje de precisión de más o menos :						
	0.50	0.75	1.00	1.25	1.50	1.75	2.00
5000	1489	793	479	317	225	167	129
5500	1530	804	483	319	226	167	129
6000	1567	814	487	321	226	168	129
6500	1599	823	490	322	227	168	129
7000	1628	830	493	323	228	169	130
7500	1653	837	495	324	228	169	130
8000	1676	843	497	325	228	169	130
8500	1697	848	499	326	229	169	130
9000	1716	853	500	327	229	169	130
9500	1734	857	502	327	230	170	130
10000	1750	861	503	328	230	170	130
11000	1778	868	505	329	230	170	131
12000	1802	874	507	330	231	170	131
13000	1823	879	509	330	231	170	131
14000	1842	883	511	331	231	171	131
15000	1858	887	512	331	232	171	131
16000	1873	890	513	332	232	171	131
17000	1886	893	514	332	232	171	131
18000	1897	895	515	333	232	171	131
19000	1908	898	515	333	232	171	131
20000	1918	900	516	333	232	171	131
22500	1938	904	518	334	233	171	131
25000	1955	908	519	334	233	171	131
27500	1969	911	520	335	233	172	131
30000	1981	914	521	335	233	172	132
32500	1991	916	521	335	234	172	132
35000	2000	918	522	336	234	172	132
37500	2007	919	522	336	234	172	132
40000	2014	921	523	336	234	172	132
42500	2020	922	523	336	234	172	132
45000	2026	923	524	336	234	172	132
47500	2030	924	524	337	234	172	132
50000	2035	925	524	337	234	172	132
55000	2042	927	525	337	234	172	132
60000	2049	928	525	337	234	172	132
65000	2054	929	526	337	234	172	132
70000	2059	930	526	337	234	172	132
75000	2063	931	526	337	234	172	132
80000	2066	931	526	338	235	172	132

Tamaños de la muestra para el muestreo de atributos.
 Tasa de error esperada no mayor de 2%
 Nivel de confianza de 90 %

Tamaño de la Población	Tamaño de muestra correspondiente a un porcentaje de precisión de más o menos :						
	0.50	0.75	1.00	1.25	1.50	1.75	2.00
85000	2069	932	527	338	235	172	132
90000	2072	933	527	338	235	172	132
95000	2075	933	527	338	235	172	132
100000	2077	934	527	338	235	172	132
110000	2081	934	527	338	235	172	132
120000	2084	935	528	338	235	172	132
130000	2087	936	528	338	235	172	132
140000	2089	936	528	338	235	172	132
150000	2091	937	528	338	235	172	132
160000	2093	937	528	338	235	172	132
170000	2095	937	528	338	235	173	132
180000	2096	937	528	338	235	173	132
190000	2098	938	528	338	235	173	132
200000	2099	938	528	338	235	173	132
250000	2103	939	529	338	235	173	132
300000	2106	939	529	339	235	173	132
350000	2108	940	529	339	235	173	132
400000	2110	940	529	339	235	173	132
450000	2111	940	529	339	235	173	132
500000	2112	941	529	339	235	173	132

Tamaños de muestra para el muestreo de atributos.
Tasa de error esperada no mayor de 2%
Nivel de confianza de 95 %

Tamaño de la Población	Tamaño de muestra correspondiente a un porcentaje de precisión de más o menos :						
	0.50	0.75	1.00	1.25	1.50	1.75	2.00
50	49	48	46	45	43	41	39
100	96	93	88	82	76	71	65
150	142	134	125	114	103	93	83
200	187	174	158	141	125	110	96
250	230	210	187	164	143	123	107
300	272	245	214	184	158	135	115
350	313	277	238	202	171	144	122
400	353	307	261	218	182	152	128
450	391	336	281	232	191	158	132
500	428	364	300	245	200	164	136
550	465	389	317	256	208	169	140
600	500	414	333	267	214	174	143
650	534	437	348	276	220	178	145
700	567	459	362	285	226	181	148
750	600	480	375	293	231	185	150
800	632	500	387	300	235	188	152
850	662	519	399	307	240	190	154
900	692	538	409	313	243	193	155
950	722	555	420	319	247	195	157
1000	750	572	429	325	250	197	158
1100	805	603	446	335	256	200	160
1200	858	632	462	343	261	204	162
1300	908	659	476	351	266	206	164
1400	955	684	489	358	270	209	165
1500	1001	707	501	364	273	211	167
1600	1044	728	512	370	276	213	168
1700	1086	748	521	375	279	214	169
1800	1126	767	530	380	282	216	170
1900	1165	785	539	384	284	217	171
2000	1201	801	547	388	286	218	172
2250	1287	839	564	396	291	221	173
2500	1366	871	578	404	295	223	175
2750	1437	900	591	410	298	225	176
3000	1502	925	601	415	301	227	177
3250	1563	948	611	419	303	228	177
3500	1618	968	619	423	305	229	178
3750	1670	986	627	427	307	230	179
4000	1718	1002	633	430	308	231	179
4250	1762	1017	639	432	310	232	180
4500	1804	1031	645	435	311	233	180

Tamaños de muestra para el muestreo de atributos.
Tasa de error esperada no mayor de 2%
Nivel de confianza de 95 %

Tamaño de la Población	Tamaño de muestra correspondiente a un porcentaje de precisión de más o menos :						
	0.50	0.75	1.00	1.25	1.50	1.75	2.00
4750	1843	1044	649	437	312	233	181
5000	1879	1055	654	439	313	234	181
5500	1946	1076	662	443	315	235	182
6000	2005	1094	668	446	316	236	182
6500	2058	1109	674	448	318	236	182
7000	2105	1123	679	450	319	237	183
7500	2148	1135	684	452	320	238	183
8000	2188	1146	688	454	321	238	183
8500	2223	1156	691	456	321	238	184
9000	2256	1165	694	457	322	239	184
9500	2286	1173	697	458	323	239	184
10000	2314	1180	700	459	323	239	184
11000	2364	1193	704	461	324	240	185
12000	2407	1204	708	463	325	240	185
13000	2445	1213	711	464	326	241	185
14000	2478	1221	714	465	326	241	185
15000	2508	1228	716	466	327	241	185
16000	2534	1235	719	467	327	242	186
17000	2558	1240	721	468	328	242	186
18000	2580	1245	722	469	328	242	186
19000	2599	1250	724	469	328	242	186
20000	2617	1254	725	470	329	242	186
22500	2656	1263	728	471	329	243	186
25000	2687	1270	730	472	330	243	186
27500	2714	1276	732	473	330	243	186
30000	2737	1281	734	474	330	243	187
32500	2756	1285	735	474	331	244	187
35000	2773	1289	737	475	331	244	187
37500	2787	1292	738	475	331	244	187
40000	2800	1295	739	476	331	244	187
42500	2812	1297	739	476	332	244	187
45000	2822	1299	740	476	332	244	187
47500	2832	1301	741	477	332	244	187
50000	2840	1303	741	477	332	244	187
55000	2855	1306	742	477	332	244	187
60000	2867	1309	743	478	332	244	187
65000	2878	1311	744	478	332	244	187
70000	2887	1313	744	478	333	245	187
75000	2895	1315	745	478	333	245	187
80000	2902	1316	745	479	333	245	187

Tamaños de muestra para el muestreo de atributos.
Tasa de error esperada no mayor de 2%
Nivel de confianza de 95 %

Tamaño de la Población	Tamaño de muestra correspondiente a un porcentaje de precisión de más o menos :						
	0.50	0.75	1.00	1.25	1.50	1.75	2.00
85000	2908	1317	746	479	333	245	187
90000	2914	1318	746	479	333	245	187
95000	2919	1319	747	479	333	245	187
100000	2923	1320	747	479	333	245	187
110000	2931	1322	747	479	333	245	187
120000	2938	1323	748	479	333	245	187
130000	2943	1324	748	480	333	245	187
140000	2948	1325	748	480	333	245	187
150000	2952	1326	749	480	333	245	188
160000	2956	1327	749	480	333	245	188
170000	2959	1328	749	480	333	245	188
180000	2962	1328	749	480	334	245	188
190000	2964	1329	749	480	334	245	188
200000	2967	1329	750	480	334	245	188
250000	2975	1331	750	480	334	245	188
300000	2981	1332	751	481	334	245	188
350000	2986	1333	751	481	334	245	188
400000	2989	1334	751	481	334	245	188
450000	2991	1334	751	481	334	245	188
500000	2993	1335	751	481	334	245	188

Tamaños de muestra para el muestreo de atributos.
Tasa de error esperada no mayor de 3%
Nivel de confianza de 90 %

Tamaño de la Población	Tamaño de muestra correspondiente a un porcentaje de precisión de más o menos:						
	0.50	0.75	1.00	1.25	1.50	1.75	2.00
50	49	47	43	39	35	33	31
100	96	88	77	66	55	51	46
150	143	125	104	85	68	61	55
200	188	159	127	99	77	68	60
250	231	189	145	110	83	73	64
300	273	217	161	118	88	77	67
350	314	242	174	125	92	80	69
400	354	265	186	131	95	82	71
450	393	286	196	136	98	84	73
500	431	305	205	141	100	86	74
550	468	323	213	144	102	87	75
600	503	340	221	148	104	88	76
650	538	356	227	151	105	89	77
700	572	370	233	153	106	90	77
750	605	384	238	155	107	91	78
800	637	396	243	157	108	92	78
850	669	408	247	159	109	92	79
900	699	419	251	161	110	93	79
950	729	430	255	163	111	93	80
1000	759	440	259	164	111	94	80
1100	815	458	265	166	113	95	81
1200	868	475	270	169	114	95	81
1300	920	490	275	170	114	96	81
1400	969	503	279	172	115	96	82
1500	1016	516	283	174	116	97	82
1600	1061	527	287	175	116	97	82
1700	1104	538	290	176	117	98	83
1800	1145	547	293	177	117	98	83
1900	1185	556	295	178	118	98	83
2000	1223	564	297	179	118	98	83
2250	1312	583	302	181	119	99	84
2500	1393	598	307	182	119	99	84
2750	1468	612	310	183	120	100	84
3000	1536	623	313	184	120	100	85
3250	1599	633	315	185	121	100	85
3500	1657	642	318	186	121	101	85
3750	1711	650	320	187	121	101	85
4000	1762	657	321	187	122	101	85
4250	1809	664	323	188	122	101	85
4500	1852	670	324	188	122	101	85

Tamaños de muestra para el muestreo de atributos.
Tasa de error esperada no mayor de 3%
Nivel de confianza de 90 %

Tamaño de la Población	Tamaño de muestra correspondiente a un porcentaje de precisión de más o menos :						
	0.50	0.75	1.00	1.25	1.50	1.75	2.00
4750	1893	675	325	189	122	101	85
5000	1932	680	327	189	122	102	85
5500	2002	688	329	190	123	102	86
6000	2065	696	330	190	123	102	86
6500	2121	702	332	191	123	102	86
7000	2172	707	333	191	123	102	86
7500	2218	712	334	191	123	102	86
8000	2259	716	335	192	124	102	86
8500	2298	720	336	192	124	102	86
9000	2333	724	336	192	124	102	86
9500	2365	727	337	192	124	102	86
10000	2355	729	338	193	124	103	86
11000	2448	734	339	193	124	103	86
12000	2494	738	340	193	124	103	86
13000	2535	742	340	193	124	103	86
14000	2571	745	341	194	124	103	86
15000	2603	748	341	194	124	103	86
16000	2631	750	342	194	125	103	87
17000	2657	752	342	194	125	103	87
18000	2680	754	343	194	125	103	87
19000	2701	756	343	194	125	103	87
20000	2721	757	343	194	125	103	87
22500	2763	760	344	195	125	103	87
25000	2797	763	345	195	125	103	87
27500	2826	765	345	195	125	103	87
30000	2850	767	345	195	125	103	87
32500	2871	768	346	195	125	103	87
35000	2889	770	346	195	125	103	87
37500	2905	771	346	195	125	103	87
40000	2919	772	346	195	125	103	87
42500	2932	773	347	195	125	103	87
45000	2943	773	347	196	125	103	87
47500	2953	774	347	196	125	103	87
50000	2963	775	347	196	125	103	87
55000	2979	776	347	196	125	103	87
60000	2992	777	347	196	125	103	87
65000	3004	778	348	196	125	103	87
70000	3014	778	348	196	125	103	87
75000	3022	779	348	196	125	103	87
80000	3030	779	348	196	125	103	87

Tamaños de muestra para el muestreo de atributos.
Tasa de error esperada no mayor de 3%
Nivel de confianza de 90 %

Tamaño de la Población	Tamaño de muestra correspondiente a un porcentaje de precisión de más o menos :						
	0.50	0.75	1.00	1.25	1.50	1.75	2.00
4750	1893	675	325	189	122	101	85
5000	1932	680	327	189	122	102	85
5500	2002	688	329	190	123	102	86
6000	2065	696	330	190	123	102	86
6500	2121	702	332	191	123	102	86
7000	2172	707	333	191	123	102	86
7500	2218	712	334	191	123	102	86
8000	2259	716	335	192	124	102	86
8500	2298	720	336	192	124	102	86
9000	2333	724	336	192	124	102	86
9500	2365	727	337	192	124	102	86
10000	2355	729	338	193	124	103	86
11000	2448	734	339	193	124	103	86
12000	2494	738	340	193	124	103	86
13000	2535	742	340	193	124	103	86
14000	2571	745	341	194	124	103	86
15000	2603	748	341	194	124	103	86
16000	2631	750	342	194	125	103	87
17000	2657	752	342	194	125	103	87
18000	2680	754	343	194	125	103	87
19000	2701	756	343	194	125	103	87
20000	2721	757	343	194	125	103	87
22500	2763	760	344	195	125	103	87
25000	2797	763	345	195	125	103	87
27500	2826	765	345	195	125	103	87
30000	2850	767	345	195	125	103	87
32500	2871	768	346	195	125	103	87
35000	2889	770	346	195	125	103	87
37500	2905	771	346	195	125	103	87
40000	2919	772	346	195	125	103	87
42500	2932	773	347	195	125	103	87
45000	2943	773	347	196	125	103	87
47500	2953	774	347	196	125	103	87
50000	2963	775	347	196	125	103	87
55000	2979	776	347	196	125	103	87
60000	2992	777	347	196	125	103	87
65000	3004	778	348	196	125	103	87
70000	3014	778	348	196	125	103	87
75000	3022	779	348	196	125	103	87
80000	3030	779	348	196	125	103	87

Tamaños de muestra para el muestreo de atributos.

Tasa de error esperada no mayor de 2%

Nivel de confianza de 95 %

Tamaño de la Población	Tamaño de muestra correspondiente a un porcentaje de precisión de más o menos :						
	0.50	0.75	1.00	1.25	1.50	1.75	2.00
50	49	47	45	42	39	37	35
100	97	91	83	73	64	59	55
150	145	132	115	97	81	74	67
200	191	169	141	116	94	84	76
250	236	204	166	131	104	92	82
300	281	236	187	144	112	99	87
350	324	266	205	155	118	103	91
400	367	294	221	164	123	107	94
450	408	320	236	172	127	111	97
500	449	345	249	179	131	114	99
550	489	368	261	185	134	116	101
600	529	390	271	190	137	118	102
650	567	411	281	195	140	120	104
700	605	430	290	199	142	122	105
750	642	448	298	203	144	123	106
800	678	466	306	207	146	124	107
850	714	482	313	210	147	125	108
900	749	498	320	213	149	126	109
950	783	513	326	215	150	127	109
1000	817	527	331	218	151	128	110
1100	882	554	342	222	153	130	111
1200	946	578	351	226	155	131	112
1300	1007	601	359	230	157	132	113
1400	1066	621	366	232	158	133	114
1500	1123	640	373	235	159	134	114
1600	1178	658	379	237	160	135	115
1700	1231	674	384	240	161	135	115
1800	1283	689	389	241	162	136	116
1900	1333	703	393	243	163	137	116
2000	1381	717	397	245	164	137	116
2250	1496	746	406	248	165	138	117
2500	1603	772	414	251	166	139	118
2750	1702	794	420	253	167	140	118
3000	1795	814	426	255	168	140	119
3250	1882	831	430	257	169	141	119
3500	1963	847	435	258	170	141	119
3750	2039	861	438	260	170	142	120
4000	2111	873	441	261	171	142	120
4250	2178	885	444	262	171	142	120
4500	2242	895	447	263	172	143	120

Tamaños de muestra para el muestreo de atributos.
 Tasa de error esperada no mayor de 2%
 Nivel de confianza de 95 %

Tamaño de la Población	Tamaño de muestra correspondiente a un porcentaje de precisión de más o menos :						
	0.50	0.75	1.00	1.25	1.50	1.75	2.00
4750	2303	904	449	263	172	143	121
5000	2360	913	451	264	172	143	121
5500	2466	929	455	265	173	143	121
6000	2562	942	458	267	173	144	121
6500	2649	953	461	267	174	144	121
7000	2728	963	463	268	174	144	122
7500	2801	972	465	269	174	144	122
8000	2868	980	467	270	174	145	122
8500	2930	987	469	270	175	145	122
9000	2987	994	470	271	175	145	122
9500	3040	1000	472	271	175	145	122
10000	3089	1005	473	271	175	145	122
11000	3179	1014	475	272	176	145	122
12000	3257	1022	477	273	176	146	122
13000	3327	1029	478	273	176	146	123
14000	3389	1035	479	274	176	146	123
15000	3444	1040	480	274	176	146	123
16000	3494	1044	481	274	176	146	123
17000	3540	1048	482	274	177	146	123
18000	3581	1052	483	275	177	146	123
19000	3619	1055	484	275	177	146	123
20000	3654	1058	484	275	177	146	123
22500	3730	1064	486	276	177	146	123
25000	3793	1070	487	276	177	146	123
27500	3846	1074	488	276	177	147	123
30000	3891	1077	488	276	177	147	123
32500	3930	1080	489	277	177	147	123
35000	3965	1083	489	277	177	147	123
37500	3995	1085	490	277	178	147	123
40000	4022	1087	490	277	178	147	123
42500	4045	1089	491	277	178	147	123
45000	4067	1090	491	277	178	147	123
47500	4086	1092	491	277	178	147	123
50000	4104	1093	491	227	178	147	123
55000	4135	1095	492	278	178	147	123
60000	4161	1097	492	278	178	147	123
65000	4183	1099	493	278	178	147	123
70000	4203	1100	493	278	178	147	123
75000	4220	1101	493	278	178	147	124
80000	4234	1102	493	278	178	147	124

Tamaños de muestra para el muestreo de atributos.
 Tasa de error esperada no mayor de 2%
 Nivel de confianza de 95 %

Tamaño de la Población	Tamaño de muestra correspondiente a un porcentaje de precisión de más o menos :						
	0.50	0.75	1.00	1.25	1.50	1.75	2.00
85000	4248	1103	493	278	178	147	124
90000	4259	1104	494	278	178	147	124
95000	4270	1104	494	278	178	147	124
100000	4280	1105	494	278	178	147	124
110000	4296	1106	494	278	178	147	124
120000	4310	1107	494	278	178	147	124
130000	4322	1108	494	278	178	147	124
140000	4333	1109	495	278	178	147	124
150000	4342	1109	495	278	178	147	124
160000	4350	1110	495	278	178	147	124
170000	4357	1110	495	279	178	147	124
180000	4363	1111	495	279	178	147	124
190000	4368	1111	495	279	178	147	124
200000	4373	1111	495	279	178	147	124
250000	4393	1112	495	279	178	147	124
300000	4405	1113	496	279	178	147	124
350000	4415	1114	496	279	178	147	124
400000	4422	1114	496	279	178	147	124
450000	4427	1115	496	279	178	147	124
500000	4431	1115	496	279	178	147	124

Tamaños de muestra para el muestreo de atributos.
Tasa de error esperada no mayor de 2%
Nivel de confianza de 95 %

Tamaño de la Población	Tamaño de muestra correspondiente a un porcentaje de precisión de más o menos :						
	0.50	0.75	1.00	1.25	1.50	1.75	2.00
85000	4248	1103	493	278	178	147	124
90000	4259	1104	494	278	178	147	124
95000	4270	1104	494	278	178	147	124
100000	4280	1105	494	278	178	147	124
110000	4296	1106	494	278	178	147	124
120000	4310	1107	494	278	178	147	124
130000	4322	1108	494	278	178	147	124
140000	4333	1109	495	278	178	147	124
150000	4342	1109	495	278	178	147	124
160000	4350	1110	495	278	178	147	124
170000	4357	1110	495	279	178	147	124
180000	4363	1111	495	279	178	147	124
190000	4368	1111	495	279	178	147	124
200000	4373	1111	495	279	178	147	124
250000	4393	1112	495	279	178	147	124
300000	4405	1113	496	279	178	147	124
350000	4415	1114	496	279	178	147	124
400000	4422	1114	496	279	178	147	124
450000	4427	1115	496	279	178	147	124
500000	4431	1115	496	279	178	147	124

Tamaños de muestra para el muestreo de atributos.
Tasa de error esperada no mayor de 5%
Nivel de confianza de 90 %

Tamaño de la Población	Tamaño de muestra correspondiente a un porcentaje de precisión de más o menos :						
	1.00	1.50	2.00	2.50	3.00	3.50	4.00
4750	1011	509	300	197	138	102	78
5000	1022	512	301	197	138	102	79
5500	1041	517	303	198	139	102	79
6000	1058	521	305	198	139	103	79
6500	1073	525	306	199	139	103	79
7000	1085	528	307	199	139	103	79
7500	1097	530	308	200	140	103	79
8000	1107	533	308	200	140	103	79
8500	1116	535	309	200	140	103	79
9000	1124	537	310	201	140	103	79
9500	1132	538	310	201	140	103	79
10000	1138	540	311	201	140	103	79
11000	1150	543	312	201	140	103	79
12000	1161	545	312	202	141	104	79
13000	1169	547	313	202	141	104	79
14000	1177	548	314	202	141	104	79
15000	1183	550	314	202	141	104	79
16000	1189	551	315	203	141	104	79
17000	1195	552	315	203	141	104	79
18000	1199	553	315	203	141	104	79
19000	1203	554	315	203	141	104	79
20000	1207	555	316	203	141	104	80
22500	1215	557	316	203	141	104	80
25000	1222	558	317	203	142	104	80
27500	1227	559	317	204	142	104	80
30000	1232	560	317	204	142	104	80
32500	1236	561	318	204	142	104	80
35000	1239	562	318	204	142	104	80
37500	1242	562	318	204	142	104	80
40000	1245	563	318	204	142	104	80
42500	1247	563	318	204	142	104	80
45000	1249	564	319	204	142	104	80
47500	1251	564	319	204	142	104	80
50000	1253	564	319	204	142	104	80
55000	1256	565	319	204	142	104	80
60000	1258	565	319	204	142	104	80
65000	1260	566	319	205	142	104	80
70000	1262	566	319	205	142	104	80
75000	1263	566	319	205	142	104	80
80000	1265	567	320	205	142	104	80

Tamaños de muestra para el muestreo de atributos.
 Tasa de error esperada no mayor de 5%
 Nivel de confianza de 90 %

Tamaño de la Población	Tamaño de muestra correspondiente a un porcentaje de precisión de más o menos :						
	1.00	1.50	2.00	2.50	3.00	3.50	4.00
85000	1266	567	320	205	142	104	80
90000	1267	567	320	205	142	104	80
95000	1268	567	320	205	142	104	80
100000	1269	568	320	205	142	104	80
110000	1270	568	320	205	142	104	80
120000	1271	568	320	205	142	104	80
130000	1272	568	320	205	142	104	80
140000	1273	568	320	205	142	104	80
150000	1274	569	320	205	142	104	80
160000	1275	569	320	205	142	104	80
170000	1275	569	320	205	142	104	80
180000	1276	569	320	205	142	104	80
190000	1276	569	320	205	142	104	80
200000	1277	569	320	205	142	104	80
250000	1278	569	320	205	142	104	80
300000	1279	570	320	205	142	104	80
350000	1280	570	321	205	142	104	80
400000	1281	570	321	205	142	104	80
450000	1281	570	321	205	142	104	80
500000	1282	570	321	205	142	104	80

Tamaños de muestra para el muestreo de atributos.
Tasa de error esperada no mayor de 5%
Nivel de confianza de 95 %

Tamaño de la Pobla ción	Tamaño de muestra correspondiente a un porcentaje de precisión de más o menos :						
	1.00	1.50	2.00	2.50	3.00	3.50	4.00
50	48	47	45	42	40	37	34
100	94	89	82	74	66	59	53
150	138	126	112	99	86	74	64
200	180	160	139	118	100	85	72
250	219	191	161	134	111	93	78
300	257	218	180	147	120	99	82
350	293	244	198	159	128	104	86
400	328	267	213	168	134	108	88
450	360	289	226	177	139	111	90
500	392	309	238	184	144	114	92
550	422	327	249	190	148	117	94
600	451	344	259	196	151	119	95
650	479	360	268	201	154	121	97
700	505	375	276	206	157	122	98
750	531	389	283	210	159	124	98
800	556	402	290	213	161	125	99
850	579	415	296	217	163	126	100
900	602	426	302	220	165	127	101
950	624	437	308	223	167	128	101
1000	645	447	313	225	168	129	102
1100	686	466	322	230	171	131	103
1200	723	483	330	234	173	132	104
1300	759	499	337	238	175	133	104
1400	792	513	344	241	177	134	105
1500	823	526	349	244	178	135	105
1600	852	538	354	246	179	136	106
1700	880	549	359	249	181	136	106
1800	906	559	363	251	182	137	107
1900	930	568	367	253	183	138	107
2000	954	577	371	254	184	138	107
2250	1007	596	379	258	185	139	108
2500	1054	612	385	261	187	140	109
2750	1096	626	391	263	188	141	109
3000	1134	638	395	266	189	141	109
3250	1168	649	400	267	190	142	110

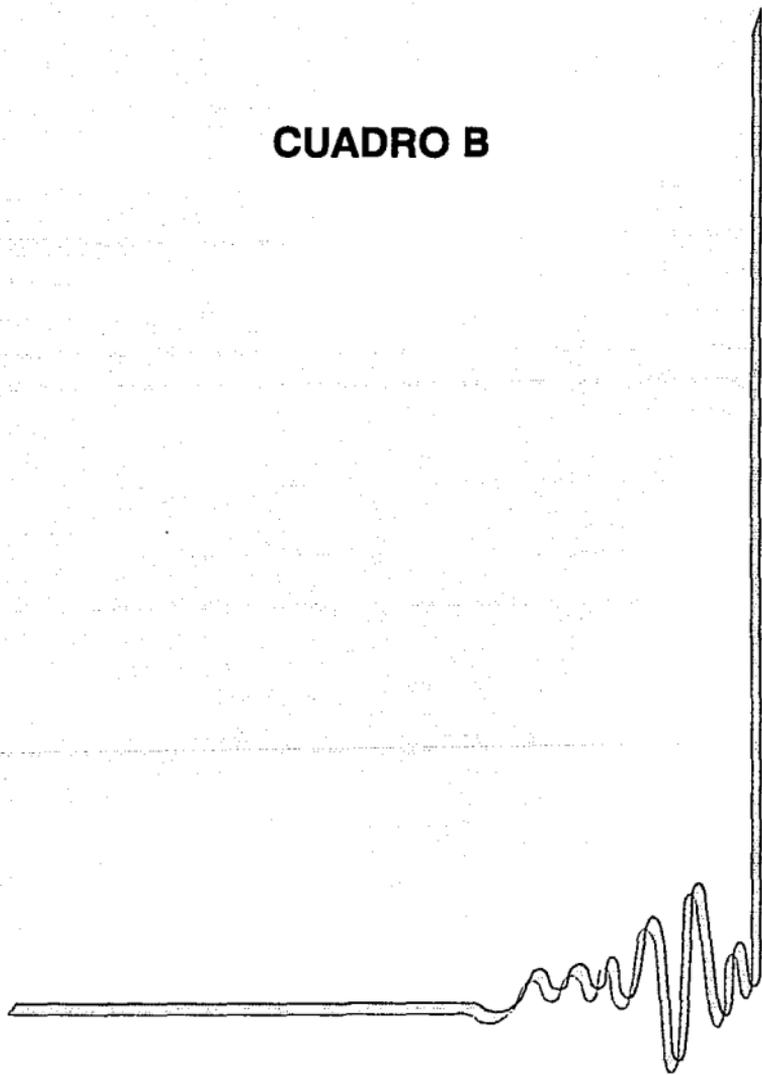
Tamaños de muestra para el muestreo de atributos.
Tasa de error esperada no mayor de 5%
Nivel de confianza de 95 %

Tamaño de la Población	Tamaño de muestra correspondiente a un porcentaje de precisión de más o menos :						
	1.00	1.50	2.00	2.50	3.00	3.50	4.00
3500	1199	658	403	269	191	142	110
3750	1227	666	406	270	192	143	110
4000	1253	674	409	272	192	143	110
4250	1276	681	411	273	193	143	111
4500	1298	687	414	274	194	144	111
4750	1318	692	416	275	194	144	111
5000	1336	697	418	275	194	144	111
5500	1370	706	421	277	195	145	111
6000	1399	714	423	278	196	145	111
6500	1424	721	426	279	196	145	112
7000	1447	726	428	280	197	145	112
7500	1467	731	430	281	197	146	112
8000	1485	736	431	281	197	146	112
8500	1502	740	432	282	198	146	112
9000	1517	743	434	282	198	146	112
9500	1530	747	435	283	198	146	112
10000	1543	750	436	283	198	146	112
11000	1565	755	438	284	199	146	112
12000	1583	759	439	285	199	147	112
13000	1600	763	440	285	199	147	113
14000	1614	766	441	285	199	147	113
15000	1626	769	442	286	200	147	113
16000	1637	771	443	286	200	147	113
17000	1647	774	444	287	200	147	113
18000	1656	776	444	287	200	147	113
19000	1664	777	445	287	200	147	113
20000	1672	779	446	287	200	147	113
22500	1687	782	447	288	200	147	113
25000	1700	785	448	288	201	148	113
27500	1711	787	448	288	201	148	113
30000	1720	789	449	289	201	148	113
32500	1727	791	449	289	201	148	113
35000	1734	792	450	289	201	148	113
37500	1740	793	450	289	201	148	113
40000	1745	794	451	289	201	148	113
42500	1749	795	451	289	201	148	113
45000	1753	796	451	290	201	148	113
47500	1757	797	451	290	201	148	113
50000	1760	798	452	290	201	148	113
55000	1766	799	452	290	202	148	113

Tamaños de muestra para el muestreo de atributos.
Tasa de error esperada no mayor de 5%
Nivel de confianza de 95 %

Tamaño de la Población	Tamaño de muestra correspondiente a un porcentaje de precisión de más o menos :						
	1.00	1.50	2.00	2.50	3.00	3.50	4.00
60000	1770	800	452	290	202	148	113
65000	1774	801	453	290	202	148	113
70000	1778	801	453	290	202	148	113
75000	1781	802	453	290	202	148	113
80000	1784	802	453	290	202	148	113
85000	1786	803	453	290	202	148	113
90000	1788	803	453	291	202	148	113
95000	1790	804	454	291	202	148	113
100000	1792	804	454	291	202	148	113
110000	1794	805	454	291	202	148	113
120000	1797	805	454	291	202	148	113
130000	1799	805	454	291	202	148	113
140000	1801	806	454	291	202	148	113
150000	1802	806	454	291	202	148	113
160000	1804	806	454	291	202	148	113
170000	1805	807	454	291	202	148	113
180000	1806	807	455	291	202	148	113
190000	1907	807	455	291	202	148	113
200000	1808	807	455	291	202	148	113
250000	1811	808	455	291	202	148	113
300000	1813	808	455	291	202	148	114
350000	1815	809	455	291	202	148	114
400000	1816	809	455	291	202	148	114
450000	1817	809	455	291	202	148	114
500000	1818	809	455	291	202	148	114

CUADRO B



Tamaños de la muestra para el muestreo de variables.
 Tamaño de muestra necesario para un
 Nivel de confianza (en porcentaje) de :

Razón de error
 de muestreo a
 desviación
 estándar

	75	80	85	90	95	98	99
--	----	----	----	----	----	----	----

l(*)

Tamaño de la población : 5000

0.01	3630	3834	4028	4221	4425	4578	4650
0.02	1992	2255	2544	2876	3289	3652	3842
0.03	1137	1338	1577	1878	2303	2731	2979
0.04	710	852	1029	1264	1623	2018	2267
0.05	479	581	711	890	1176	1512	1733
0.06	343	419	517	654	880	1157	1347
0.07	257	315	390	498	678	905	1065
0.08	199	245	305	390	536	724	859
0.09	159	195	244	314	434	590	704
0.10	129	160	199	257	357	489	586
0.11	108	133	166	215	299	411	494
0.12	91	112	140	182	254	350	422
0.13	78	96	120	156	218	302	364
0.14	67	83	104	135	189	262	317
0.15	59	72	91	118	166	230	279
0.16	52	64	80	104	146	203	247
0.17	46	57	71	92	130	181	220
0.18	41	51	64	83	116	162	197
0.19	37	46	57	74	105	146	178
0.20	33	41	52	67	95	132	161
0.21	30	37	47	61	86	120	146
0.22	28	34	43	56	79	110	134
0.23	25	31	39	51	72	101	123
0.24	23	29	36	47	66	93	113
0.25	22	27	33	43	61	86	104
0.30	15	19	23	30	43	60	73
0.35	11	14	17	22	32	44	54
0.40	9	11	13	17	24	34	42

l(*) Fuente : Lockheed-Georgia Company, Grupo de Análisis Matemático

Tamaños de la muestra para el muestreo de variables.
 Tamaño de muestra necesario para un
 Nivel de confianza (en porciento) de :

Razón de error de muestreo a desviación estándar	75	80	85	90	95	98	99
Tamaño de la población : 6000							
0.01	4129	4395	4653	4912	5190	5402	5503
0.02	2133	2439	2780	3180	3693	4158	4406
0.03	1182	1400	1664	2003	2495	3004	3307
0.04	728	877	1065	1320	1715	2164	2452
0.05	487	593	729	917	1224	1592	1840
0.06	347	425	526	668	906	1203	1410
0.07	259	318	395	506	694	934	1105
0.08	200	247	308	395	546	742	884
0.09	160	197	246	317	440	602	721
0.10	130	160	201	259	362	497	598
0.11	108	133	167	216	302	417	503
0.12	91	112	141	183	256	354	428
0.13	78	96	121	156	220	305	369
0.14	67	83	104	135	190	265	321
0.15	59	73	91	118	167	232	281
0.16	52	64	80	104	147	205	249
0.17	46	57	71	93	131	182	221
0.18	41	51	64	83	117	163	198
0.19	37	46	57	75	105	147	179
0.20	33	41	52	67	95	133	162
0.21	30	38	47	61	86	121	147
0.22	28	34	43	56	79	110	134
0.23	25	31	39	51	72	101	123
0.24	23	29	36	47	66	93	113
0.25	22	27	33	43	61	86	105
0.30	15	19	23	30	43	60	73
0.35	11	14	17	23	32	44	54
0.40	9	11	13	17	24	34	42

Tamaños de la muestra para el muestreo de variables.
 Tamaño de muestra necesario para un
 Nivel de confianza (en porciento) de :

Razón de error de muestreo a desviación estándar	75	80	85	90	95	98	99
Tamaño de la población : 7000							
0.01	4579	4909	5233	5562	5922	6199	6332
0.02	2247	2589	2977	3441	4049	4614	4922
0.03	1216	1448	1733	2104	2652	3236	3590
0.04	740	896	1093	1363	1788	2281	2604
0.05	493	601	741	938	1261	1654	1924
0.06	350	429	532	679	926	1238	1459
0.07	261	320	399	512	706	955	1134
0.08	201	248	310	399	553	755	903
0.09	160	198	247	319	445	611	733
0.10	130	161	202	261	365	503	606
0.11	108	134	168	217	304	421	509
0.12	91	113	141	184	257	357	433
0.13	78	96	121	157	221	307	372
0.14	67	83	105	136	191	266	323
0.15	59	73	91	119	167	233	283
0.16	52	64	80	105	147	206	250
0.17	46	57	71	93	131	183	223
0.18	41	51	64	83	117	164	199
0.19	37	46	57	75	105	147	179
0.20	33	41	52	68	95	133	162
0.21	30	38	47	61	87	121	148
0.22	28	34	43	56	79	111	135
0.23	25	31	39	51	72	101	124
0.24	23	29	36	47	67	93	114
0.25	22	27	33	44	61	86	105
0.30	15	19	23	30	43	60	73
0.35	11	14	17	23	32	44	54
0.40	9	11	13	17	24	34	42

Tamaños de la muestra para el muestreo de variables.

Tamaño de muestra necesario para un
Nivel de confianza (en porcentaje) de :

Razón de error
de muestreo a
desviación

estándar 75 80 85 90 95 98 99

Tamaño de la población : 8000

0.01	4987	5381	5772	6175	6622	6970	7139
0.02	2341	2714	3144	3666	4365	5028	5396
0.03	1243	1487	1784	2186	2784	3434	3836
0.04	750	910	1115	1397	1847	2378	2730
0.05	497	608	751	954	1290	1705	1992
0.06	352	432	537	688	942	1266	1498
0.07	262	322	402	517	715	971	1158
0.08	202	249	312	402	559	765	918
0.09	161	198	248	321	448	617	743
0.10	131	161	202	262	367	508	613
0.11	108	134	168	218	306	424	513
0.12	91	113	142	184	259	360	436
0.13	78	97	121	157	222	308	375
0.14	67	83	105	136	192	267	325
0.15	59	73	92	119	168	234	285
0.16	52	64	81	105	148	207	251
0.17	46	57	72	93	131	184	224
0.18	41	51	64	83	117	164	200
0.19	37	46	57	75	106	148	180
0.20	33	41	52	68	95	134	163
0.21	30	38	47	61	87	121	148
0.22	28	34	43	56	79	111	135
0.23	25	31	39	51	72	102	124
0.24	23	29	36	47	67	93	114
0.25	22	27	34	44	61	86	105
0.30	15	19	23	30	43	60	74
0.35	11	14	17	23	32	44	54
0.40	9	11	13	17	24	34	42

Tamaños de la muestra para el muestreo de variables.
Tamaño de muestra necesario para un
Nivel de confianza (en porcentaje) de :

Razón de error de muestreo a desviación estándar	75	80	85	90	95	98	99
Tamaño de la población : 9000							
0.01	5358	5815	6275	6754	7292	7718	7925
0.02	2420	2821	3288	3863	4647	5406	5834
0.03	1265	1518	1833	2254	2896	3606	4052
0.04	758	922	1132	1424	1896	2460	2838
0.05	501	613	759	967	1313	1746	2049
0.06	354	435	541	694	954	1289	1529
0.07	263	324	404	521	722	985	1177
0.08	203	250	313	404	563	774	930
0.09	161	199	249	323	451	623	751
0.10	131	162	203	263	369	511	618
0.11	109	134	169	219	307	427	517
0.12	91	113	142	185	260	361	439
0.13	78	97	121	158	222	310	376
0.14	68	84	105	136	192	268	327
0.15	59	73	92	119	168	235	286
0.16	52	64	81	105	148	207	252
0.17	46	57	72	93	131	184	224
0.18	41	51	64	83	118	165	201
0.19	37	46	58	75	106	148	181
0.20	33	41	52	68	96	134	163
0.21	30	38	47	61	87	122	148
0.22	28	34	43	56	79	111	135
0.23	25	31	39	51	73	102	124
0.24	23	29	36	47	67	94	114
0.25	22	27	34	44	62	86	105
0.30	15	19	23	30	43	60	74
0.35	11	14	17	23	32	44	54
0.40	9	11	13	17	24	34	42

Tamaños de la muestra para el muestreo de variables.

Tamaño de muestra necesario para un
Nivel de confianza (en porcentaje) de :Razón de error
de muestreo a
desviación
estándar

75 80 85 90 95 98 99

Tamaño de la población : 10000

0.01	5697	6217	6745	7302	7935	8441	8690
0.02	2487	2912	3412	4036	4900	5751	6238
0.03	1283	1544	1872	2312	2992	3756	4243
0.04	765	932	1147	1447	1937	2529	2930
0.05	503	617	766	977	1332	1780	2097
0.06	355	437	545	700	965	1308	1556
0.07	264	325	406	524	728	995	1192
0.08	203	251	314	406	567	780	939
0.09	161	199	250	324	453	627	757
0.10	131	162	203	264	370	514	622
0.11	109	134	169	219	308	429	520
0.12	92	113	142	185	260	363	441
0.13	78	97	122	158	223	311	378
0.14	68	84	105	137	193	269	328
0.15	59	73	92	119	168	235	287
0.16	52	64	81	105	148	208	253
0.17	46	57	72	93	132	184	225
0.18	41	51	64	83	118	165	201
0.19	37	46	58	75	106	148	181
0.20	33	41	52	68	96	134	164
0.21	30	38	47	61	87	122	149
0.22	28	34	43	56	79	111	136
0.23	25	31	40	51	73	102	124
0.24	23	29	36	47	67	94	114
0.25	22	27	34	44	62	86	105
0.30	15	19	23	30	43	60	74
0.35	11	14	17	23	32	44	54
0.40	9	11	13	17	24	34	42

Tamaños de la muestra para el muestreo de variables.
 Tamaño de muestra necesario para un
 Nivel de confianza (en porcentaje) de :

Razón de error de muestreo a desviación estándar	75	80	85	90	95	98	99
Tamaño de la población : 12500							
0.01	6429	7099	7796	8551	9432	10156	10518
0.02	2617	3092	3662	4390	5432	6499	7127
0.03	1316	1593	1944	2424	3182	4061	4636
0.04	776	949	1174	1490	2015	2663	3113
0.05	508	625	778	997	1369	1846	2189
0.06	358	441	551	710	984	1343	1606
0.07	265	327	409	529	738	1016	1222
0.08	204	252	316	409	573	793	957
0.09	162	200	251	326	457	635	769
0.10	131	163	204	265	373	519	630
0.11	109	135	169	220	310	432	525
0.12	92	114	143	186	262	365	445
0.13	78	97	122	159	224	313	381
0.14	68	84	105	137	193	271	330
0.15	59	73	92	120	169	237	288
0.16	52	64	81	105	149	208	254
0.17	46	57	72	93	132	185	226
0.18	41	51	64	83	118	165	202
0.19	37	46	58	75	106	149	182
0.20	34	41	52	68	96	134	164
0.21	30	38	47	62	87	122	149
0.22	28	34	43	56	79	111	136
0.23	25	31	44	51	73	102	125
0.24	23	29	36	47	67	94	115
0.25	22	27	34	44	62	87	106
0.30	15	19	23	30	43	60	74
0.35	11	14	17	23	32	45	54
0.40	9	11	13	17	24	34	42

Tamaños de la muestra para el muestreo de variables.
 Tamaño de muestra necesario para un
 Nivel de confianza (en porciento) de :

Razón de error
 de muestreo a
 desviación
 estándar

	75	80	85	90	95	98	99
Tamaño de la población : 15000							
0.01	7032	7841	8701	9651	10788	11746	12233
0.02	2712	3225	3850	4663	5856	7115	7875
0.03	1340	1628	1996	2505	3323	4294	4941
0.04	785	961	1192	1520	2070	2761	3248
0.05	512	630	786	1010	1394	1893	2254
0.06	359	443	555	710	997	1367	1641
0.07	266	328	412	533	746	1030	1242
0.08	205	253	317	412	578	801	970
0.09	162	201	252	327	460	640	777
0.10	132	163	205	266	375	523	635
0.11	109	135	170	221	311	435	579
0.12	92	114	143	186	263	367	447
0.13	78	97	122	159	224	314	383
0.14	68	84	105	137	194	272	331
0.15	59	73	92	120	169	237	290
0.16	52	64	81	105	149	209	255
0.17	46	57	72	94	132	186	226
0.18	41	51	64	84	118	166	202
0.19	37	46	58	75	106	149	182
0.20	34	41	52	68	96	135	164
0.21	30	38	47	62	87	122	149
0.22	28	34	43	56	79	112	136
0.23	25	31	40	51	73	102	125
0.24	23	29	36	47	67	94	115
0.25	22	27	34	44	62	87	106
0.30	15	19	23	31	43	60	74
0.35	11	14	17	23	32	45	54
0.40	9	11	13	17	24	34	42

Tamaños de la muestra para el muestreo de variables.
 Tamaño de muestra necesario para un
 Nivel de confianza (en porciento) de :

Razón de error
 de muestreo a
 desviación
 estándar

	75	80	85	90	95	98	99
Tamaño de la población : 20000							
0.01	7966	9020	10176	11501	13153	14605	15366
0.02	2840	3408	4114	5056	6489	8072	9065
0.03	1370	1673	2065	2614	3518	4625	5385
0.04	795	977	1217	1560	2144	2894	3433
0.05	516	637	796	1027	1428	1954	2342
0.06	362	447	560	725	1014	1394	1687
0.07	267	330	415	538	755	1047	1263
0.08	205	254	319	415	583	812	986
0.09	163	201	253	329	464	647	787
0.10	132	163	206	267	377	528	642
0.11	109	135	170	222	313	438	53
0.12	92	114	143	187	264	370	451
0.13	79	97	122	159	225	316	385
0.14	68	84	106	138	195	273	333
0.15	59	73	92	120	170	238	291
0.16	52	64	81	106	149	210	256
0.17	46	57	72	94	133	186	227
0.18	41	51	64	84	118	166	203
0.19	37	46	58	75	106	149	183
0.20	34	41	52	68	99	135	165
0.21	30	38	47	62	87	123	150
0.22	28	34	43	56	80	112	137
0.23	25	32	40	52	73	102	125
0.24	23	29	36	47	67	94	115
0.25	22	27	34	44	62	87	106
0.30	15	19	23	31	43	60	74
0.35	11	14	17	23	32	45	54
0.40	9	11	13	17	24	34	42

Tamaño de la muestra para el muestreo de variables.
 Tamaño de muestra necesario para un
 Nivel de confianza (en porciento) de :

Razón de error de muestreo a desviación estándar	75	80	85	90	95	98	99
Tamaño de la población : 25000							
0.01	8655	9914	11329	12995	15145	17103	18155
0.02	2923	3528	4291	5325	6939	8781	9968
0.03	1390	1702	2108	2684	3646	4849	5691
0.04	801	987	1231	1585	2191	2981	3555
0.05	519	641	803	1038	1448	1993	2398
0.06	363	449	563	730	1024	1419	1716
0.07	268	331	416	541	761	1059	1284
0.08	206	255	320	416	587	819	995
0.09	163	202	254	330	466	651	793
0.10	132	164	206	268	379	530	646
0.11	109	136	171	222	314	440	537
0.12	92	114	144	187	264	371	453
0.13	79	97	122	160	226	317	387
0.14	68	84	106	138	195	274	334
0.15	59	73	92	120	170	239	292
0.16	52	65	81	106	150	210	257
0.17	46	57	72	94	133	186	228
0.18	41	51	64	84	119	166	203
0.19	37	46	58	75	106	150	183
0.20	34	42	52	68	96	135	165
0.21	30	38	47	62	87	123	150
0.22	28	34	43	56	80	112	137
0.23	25	32	40	52	73	102	125
0.24	23	29	36	47	67	94	115
0.25	22	27	34	44	62	87	106
0.30	15	19	23	31	43	61	74
0.35	11	14	17	23	32	45	55
0.40	9	11	13	17	24	34	42

Tamaños de la muestra para el muestreo de variables.
 Tamaño de muestra necesario para un
 Nivel de confianza (en porciento) de :

Razón de error
 de muestreo a
 desviación
 estándar

	75	80	85	90	95	98	99
Tamaño de la población : 30000							
0.01	9185	10615	12255	14228	16846	19303	20655
0.02	2981	3613	4417	5521	7276	9327	10677
0.03	1402	1721	2138	2733	3737	5011	5915
0.04	806	993	1242	1602	2224	3041	3642
0.05	521	644	807	1045	1462	2020	2437
0.06	364	450	565	734	1031	1432	1736
0.07	268	332	417	543	765	1066	1295
0.08	206	255	321	417	589	823	1002
0.09	163	202	254	331	467	654	797
0.10	132	164	206	269	380	532	649
0.11	109	136	171	222	315	441	539
0.12	92	114	144	187	265	372	454
0.13	79	97	123	160	226	317	388
0.14	68	84	106	138	195	274	335
0.15	59	73	92	120	170	239	292
0.16	52	65	81	106	150	210	257
0.17	46	57	72	94	133	187	228
0.18	41	51	64	84	119	167	204
0.19	37	46	58	75	107	150	183
0.20	34	42	52	68	96	135	165
0.21	30	38	47	62	87	123	150
0.22	28	34	43	56	80	112	137
0.23	26	32	40	52	73	102	125
0.24	23	29	36	47	67	94	115
0.25	22	27	34	44	62	87	106
0.30	15	19	23	31	43	61	74
0.35	11	14	17	23	32	45	55
0.40	9	11	13	17	24	34	42

Tamaños de la muestra para el muestreo de variables.

Tamaño de muestra necesario para un
Nivel de confianza (en porciento) de:

Razón de error
de muestreo a
desviación
estándar

75 80 85 90 95 98 99

Tamaño de la población : 40000

0.01	9946	11646	13648	16141	19597	23004	24950
0.07	3057	3725	4586	5787	7745	10113	11720
0.03	1419	1746	2177	2797	3857	5229	6222
0.04	811	1002	1255	1623	2266	3120	3756
0.05	523	647	812	1054	1480	2055	2488
0.06	365	452	568	738	1040	1450	1761
0.07	269	333	419	545	769	1076	1309
0.08	206	256	322	419	592	829	1010
0.09	163	202	255	332	469	658	803
0.10	132	164	207	269	381	535	653
0.11	110	136	171	223	315	443	541
0.12	92	114	144	188	266	373	456
0.13	79	97	123	160	227	318	389
0.14	68	84	106	138	196	275	336
0.15	59	73	92	120	171	240	293
0.16	52	65	81	106	150	211	258
0.17	46	57	72	94	133	187	229
0.18	41	51	64	84	119	167	204
0.19	37	46	58	75	107	150	183
0.20	34	42	52	68	96	135	166
0.21	30	38	47	62	87	123	150
0.22	28	34	43	56	80	112	137
0.23	26	32	40	52	73	103	125
0.24	23	29	36	47	67	94	115
0.25	22	27	34	44	62	87	106
0.30	15	19	24	31	43	61	74
0.35	11	14	17	23	32	45	55
0.40	9	11	13	17	24	34	42

Tamaños de la muestra para el muestreo de variables.
 Tamaño de muestra necesario para un
 Nivel de confianza (en porciento) de :

Razón de error de muestreo a desviación estándar	75	80	85	90	95	98	99
Tamaño de la población : 50000							
0.01	10466	12366	14648	17558	21725	25993	28506
0.02	3104	3796	4693	5959	8057	10651	12450
0.03	1429	1761	2201	2837	3933	5370	6422
0.04	814	1007	1263	1636	2291	3170	3827
0.05	524	649	816	1060	1491	2076	2519
0.06	365	453	569	741	1045	1460	1777
0.07	269	334	420	547	772	1081	1318
0.08	206	256	322	420	594	832	1016
0.09	163	202	255	332	470	660	806
0.10	133	164	207	270	382	536	655
0.11	110	136	171	223	316	444	543
0.12	92	114	144	188	266	374	457
0.13	79	98	123	160	227	319	390
0.14	68	84	106	138	196	275	337
0.15	59	73	92	120	171	240	293
0.16	52	65	81	106	150	211	258
0.17	46	57	72	94	133	187	229
0.18	41	51	64	84	119	167	204
0.19	37	46	58	75	107	150	184
0.20	34	42	52	68	96	135	166
0.21	30	38	47	62	87	123	150
0.22	28	34	43	56	80	112	137
0.23	26	32	40	52	73	103	126
0.24	23	29	36	47	67	94	115
0.25	22	27	34	44	62	87	106
0.30	15	19	24	31	43	61	74
0.35	11	14	17	23	32	45	55
0.40	9	11	13	17	24	34	42

Tamaños de la muestra para el muestreo de variables.
 Tamaño de muestra necesario para un
 Nivel de confianza (en porciento) de :

Razón de error
 de muestreo a
 desviación
 estándar

	75	80	85	90	95	98	99
Tamaño de la población : 60000							
0.01	10845	12897	15400	18650	23421	28459	31498
0.02	3137	3844	4768	6080	8279	11043	12989
0.03	1436	1772	2217	2864	3985	5467	6562
0.04	817	1010	1268	1645	2309	3203	3877
0.05	525	650	818	1064	1499	2090	2540
0.06	366	453	570	743	1049	1467	1787
0.07	269	334	420	548	774	1085	1324
0.08	207	256	322	420	595	835	1019
0.09	163	203	255	333	471	661	808
0.10	133	164	207	270	382	537	656
0.11	110	136	171	223	316	445	544
0.12	92	114	144	188	266	374	457
0.13	79	98	123	160	227	319	390
0.14	68	84	106	138	196	275	337
0.15	59	73	92	121	171	240	294
0.16	52	65	81	106	150	211	258
0.17	46	57	72	94	133	187	229
0.18	41	51	64	84	119	167	204
0.19	37	46	58	75	107	150	184
0.20	34	42	52	68	96	136	166
0.21	30	38	47	62	87	123	150
0.22	28	34	43	56	80	112	137
0.23	26	32	40	52	73	103	126
0.24	23	29	36	47	67	94	115
0.25	22	27	34	44	62	87	106
0.30	15	19	24	31	43	61	74
0.35	11	14	17	23	32	45	55
0.40	9	11	13	17	25	34	42

Tamaños de la muestra para el muestreo de variables.
 Tamaño de muestra necesario para un
 Nivel de confianza (en porciento) de :

Razón de error de muestreo a desviación estándar	75	80	85	90	95	98	99
Tamaño de la población : 70000							
0.01	11132	13306	15986	19516	24804	30527	34052
0.02	3160	3880	4823	6169	8446	11342	13403
0.03	1441	1779	2229	2883	4024	5540	6666
0.04	818	1012	1272	1652	2322	3228	3913
0.05	526	651	849	1066	1504	2101	2556
0.06	366	454	571	744	1052	1473	1795
0.07	270	334	421	548	776	1088	1328
0.08	207	256	323	421	596	836	1021
0.09	164	203	255	333	472	663	810
0.10	133	164	207	270	383	538	657
0.11	110	136	171	223	317	445	544
0.12	92	114	144	188	266	374	458
0.13	79	98	123	160	227	319	391
0.14	68	84	106	138	196	276	337
0.15	59	73	92	121	171	240	294
0.16	52	65	81	106	150	211	259
0.17	46	57	72	94	133	187	229
0.18	41	51	64	84	119	167	205
0.19	37	46	58	75	107	150	184
0.20	34	42	52	68	96	136	166
0.21	31	38	47	62	88	123	151
0.22	28	34	43	56	80	112	137
0.23	26	32	40	52	73	103	126
0.24	23	29	36	47	67	94	115
0.25	22	27	34	44	62	87	106
0.30	15	19	24	31	43	61	74
0.35	11	14	17	23	32	45	55
0.40	9	11	13	17	25	34	42

Tamaños de la muestra para el muestreo de variables.
 Tamaño de muestra necesario para un
 Nivel de confianza (en porcentaje) de :

Razón de error de muestreo a desviación estándar	75	80	85	90	95	98	99
Tamaño de la población : 80000							
0.01	11358	13629	16455	20221	25954	32287	32257
0.02	3178	3907	4865	6238	8575	11576	13732
0.03	1445	1785	2238	2898	4053	5595	6747
0.04	819	1014	1275	1657	2332	3247	3941
0.05	526	652	821	1068	1508	2109	2568
0.06	366	454	572	745	1054	1477	1801
0.07	270	334	421	549	777	1090	1331
0.08	207	256	323	421	596	838	1023
0.09	164	203	255	333	472	663	811
0.10	133	164	207	270	383	538	658
0.11	110	136	171	224	317	445	545
0.12	92	114	144	188	266	375	458
0.13	79	98	123	160	227	320	391
0.14	68	84	106	138	196	276	337
0.15	59	73	92	121	171	240	294
0.16	52	65	81	106	150	211	259
0.17	46	57	72	94	133	187	229
0.18	41	51	64	84	119	167	205
0.19	37	46	58	75	107	150	184
0.20	34	42	52	68	96	136	166
0.21	31	38	47	62	88	123	151
0.22	28	34	43	56	80	112	137
0.23	26	32	40	52	73	103	126
0.24	23	29	36	47	67	94	115
0.25	22	27	34	44	62	87	106
0.30	15	19	24	31	43	61	74
0.35	11	14	17	23	32	45	55
0.40	9	11	13	17	25	34	42

Tamaños de la muestra para el muestreo de variables.
 Tamaño de muestra necesario para un
 Nivel de confianza (en porcentaje) de :

Razón de error
 de muestreo a
 desviación
 estándar

75 80 85 90 95 98 99

Tamaño de la población : 90000

0.01	11540	13892	16840	20805	26924	33803	38179
0.02	3192	3928	4898	6293	8678	11765	13999
0.03	1448	1790	2245	2910	4076	5639	6810
0.04	820	1016	1277	1661	2339	3261	3962
0.05	527	653	822	1070	1511	2115	2577
0.06	367	455	572	746	1055	1480	1805
0.07	270	335	421	549	778	1092	1334
0.08	207	256	323	421	597	838	1025
0.09	164	203	256	333	472	664	812
0.10	133	164	207	270	383	539	659
0.11	110	136	171	224	317	446	545
0.12	92	114	144	188	266	375	459
0.13	79	98	123	160	227	320	391
0.14	68	84	106	138	196	276	338
0.15	59	73	92	121	171	240	294
0.16	52	65	81	106	150	211	259
0.17	46	57	72	94	133	187	229
0.18	41	51	64	84	119	167	205
0.19	37	46	58	75	107	150	184
0.20	34	42	52	68	96	136	166
0.21	31	38	47	62	88	123	151
0.22	28	34	43	56	80	112	137
0.23	26	32	40	52	73	103	126
0.24	23	29	36	47	67	94	115
0.25	22	27	34	44	62	87	106
0.30	15	19	24	31	43	61	74
0.35	11	14	17	23	32	45	55
0.40	9	11	13	17	25	34	42

Tamaños de la muestra para el muestreo de variables.

Tamaño de muestra necesario para un

Nivel de confianza (en porciento) de :

Razón de error
de muestreo a
desviación
estándar

75 80 85 90 95 98 99

Tamaño de la población : 100000

0.01	11690	14110	17161	21298	27755	35122	39870
0.02	3204	3945	4924	6337	8763	11921	14220
0.03	1450	1793	2250	2919	4094	5674	6862
0.04	821	1017	1279	1664	2345	3273	3980
0.05	527	653	822	1071	1514	2120	2584
0.06	367	455	573	747	1056	1482	1809
0.07	270	335	421	550	778	1093	1336
0.08	207	257	323	422	597	839	1026
0.09	164	203	256	333	473	664	812
0.10	133	165	207	270	383	539	659
0.11	110	136	171	224	317	446	545
0.12	92	114	144	188	267	375	459
0.13	79	98	123	160	227	320	391
0.14	68	84	106	138	196	276	338
0.15	59	73	92	121	171	241	294
0.16	52	65	81	106	150	212	259
0.17	46	57	72	94	133	187	229
0.18	41	51	64	84	119	167	205
0.19	37	46	58	75	107	150	184
0.20	34	42	52	68	95	136	166
0.21	31	38	47	62	88	123	151
0.22	28	34	43	56	80	112	137
0.23	26	32	40	52	73	103	126
0.24	23	29	36	47	67	94	117
0.25	22	27	34	44	62	87	106
0.30	15	19	24	31	43	61	74
0.35	11	14	17	23	32	45	55
0.40	9	11	13	17	25	34	42
	75	80	85	90	95	98	99

Tamaños de la muestra para el muestreo de variables.

Tamaño de muestra necesario para un
Nivel de confianza (en porciento) de :Razón de error
de muestreo a
desviación
estándar

	75	80	85	90	95	98	99
--	----	----	----	----	----	----	----

Tamaño de la población : 500000

0.01	12896	15905	19892	25671	35676	48847	58543
0.02	3288	4074	5126	6675	9424	13178	16045
0.03	1467	1819	2292	2989	4233	5944	7261
0.04	826	1025	1292	1686	2390	3361	4111
0.05	529	657	828	1081	1532	2157	2639
0.06	368	456	575	751	1065	1500	1836
0.07	270	336	423	552	783	1103	1350
0.08	207	257	324	423	600	845	1034
0.09	164	203	256	334	474	668	818
0.10	133	165	208	271	384	541	663
0.11	110	136	172	224	318	447	548
0.12	92	115	144	188	267	376	461
0.13	79	98	123	161	228	321	393
0.14	68	84	106	139	196	277	339
0.15	59	74	93	121	171	241	295
0.16	52	65	81	106	151	212	259
0.17	46	57	72	94	133	188	230
0.18	41	51	64	84	119	168	205
0.19	37	46	58	75	107	150	184
0.20	34	42	52	68	97	136	166
0.21	31	38	47	62	88	123	151
0.22	28	34	43	56	80	112	137
0.23	26	32	40	52	73	103	126
0.24	23	29	36	47	67	94	116
0.25	22	27	34	44	62	87	107
0.30	15	19	24	31	43	61	74
0.35	11	14	17	23	32	45	55
0.40	9	11	13	17	25	34	42

Tamaños de la muestra para el muestreo de variables.

Tamaño de muestra necesario para un
Nivel de confianza (en porcentaje) de:

Razón de error de muestreo a desviación estándar	75	80	85	90	95	98	99
Tamaño de la población : 1000000							
0.01	13064	16163	20296	26348	36995	51356	62184
0.02	3299	4091	5153	6720	9513	13354	16307
0.03	1469	1822	2297	2998	4251	5980	7314
0.04	827	1026	1294	1689	2396	3373	4128
0.05	530	657	828	1082	1535	2161	2646
0.06	368	457	576	752	1066	1502	1839
0.07	271	336	423	552	784	1104	1352
0.08	207	257	324	423	600	846	1035
0.09	164	203	256	334	475	668	818
0.10	133	165	208	271	385	542	663
0.11	110	136	172	224	318	448	548
0.12	92	115	144	188	267	376	461
0.13	79	98	123	161	228	321	393
0.14	68	84	106	139	196	277	339
0.15	59	74	93	121	171	241	295
0.16	52	65	81	106	151	212	259
0.17	46	57	72	94	133	188	230
0.18	41	51	64	84	119	168	205
0.19	37	46	58	75	107	150	184
0.20	34	42	52	68	97	136	166
0.21	31	38	47	62	88	123	151
0.22	28	34	43	56	80	112	137
0.23	26	32	40	52	73	103	126
0.24	23	29	36	47	67	94	116
0.25	22	27	34	44	62	87	107
0.30	15	19	24	31	43	61	74
0.35	11	14	17	23	32	45	55
0.40	9	11	13	17	25	34	42

BIBLIOGRAFIA

Victor M. Mendivil Escalante, "Elementos de Auditoría",
Ed. Ediciones Contables y Administrativas S.A., México 1979.

Stanley D. Halper, "HandBokk of EDP Auditing",
Warren Gorham & Lamont, 1989.

"The EDP Auditor Journal",
Vol III.

Auerbach Publishers Inc., "EDP Auditing",
Bonston, M.

Departamento de Auditoría Interna, "Manual de Muestreo para Auditores",
Lockheed Aircraft Corporation.

Néstor Gonzalez Sainz, "Comunicaciones y Redes de Procesamiento de Datos",
McGraw-Hill.

Manuales de IBM :

"El Sistema/38 de IBM"
"Comunicaciones del Sistema/38 de IBM"
"Sistema/38 de IBM Equipo y Programas"

Unisys, 2200/400 System "Capabilities Overview"

Andrew S. Tanenbaum, " Computer Networks"
Prentince-Hall.

Michel F. Hordeski, "Communications Networks"
TAB Professional and Reference Books.

David Hutchison, "Local Area Network Architectures"
Addison-Wesley Publishing Company.

William Sinnema and Tom McGovern, "Digital, Analog and Data Communication",
Prentince-Hall, Inc.

Asociación Banqueros de México, "Anuario Financiero Mexicano",
Ed. Libros de México, México 1979.

Diario Oficial, 29 de octubre de 1983.

Farias G. Pedro & Pérez M. José, "Sistema Bancario Mexicano y su Evolución Hacia la Banca
Multiple",
Erografic, Offset e Imprenta, México 1979.

Perez S. Fernando V., "Síntesis de la Estructura Bancaria y del Crédito",
Ed. Trillas, México 1978.