UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

LOTERÍAS ELECTRÓNICAS A TRAVÉS DE CAJEROS AUTOMÁTICOS, LA REVOLUCIÓN EN LOS JUEGOS DE AZAR

REPORTE DE TRABAJO PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:

ACTUARIA

P R E S E N T A :

SILVIA CAMPOS RAMOS

DIRECTOR DE TESIS:
ACT. MARIBEL MERCADO REJÓN
2012

Hoja de Datos del Jurado

1. Datos del Alumno

Apellido Paterno:	Campos
Apellido Materno:	Ramos
Nombre(s):	Silvia
Teléfono:	044 55 16 78 19 62
Universidad Nacional Autónoma de México	Universidad Nacional Autónoma de México
Facultad de Ciencias	Facultad de Ciencias
Carrera:	Actuaría
Número de Cuenta:	9224543-3

2. Datos del tutor

Grado:	Actuaria
Nombre(s):	Maribel
Apellido Paterno:	Mercado
Apellido Materno:	Rejón

3. Datos del Sinodal 1

Grado:	L. en C. C.
Nombre(s):	Sergio
Apellido Paterno:	Padilla
Apellido Materno:	Reynaud

4. Datos del Sinodal 2

Grado:	Mtro.
Nombre(s):	Arturo Fernando
Apellido Paterno:	Suárez
Apellido Materno:	Flores

5. Datos del Sinodal 3

Grado:	Actuario
Nombre(s):	Daniel
Apellido Paterno:	Cid
Apellido Materno:	Padilla

6. Datos del Sinodal 4

Grado:	Actuaria
Nombre(s):	Nadia
Apellido Paterno:	Hernández
Apellido Materno:	Rebollar

7. Datos del Trabajo Escrito

Título:	Loterías Electrónicas a través de Cajeros Automáticos, la revolución en los juegos de azar
Número de Páginas:	68p
Año:	2012

Contenido

Introducción

Lotería Nacional para la Asistencia Pública es la Institución precursora de sorteos en el país, su nombre es marca de prestigio y confianza en el público consumidor de modo que un sorteo patrocinado por Lotería Nacional ante la gente inspira más confianza que algún otro que se realice mediante un canal diferente, por ejemplo la televisión o el teléfono.

A finales del 2003 Lotería Nacional lanzó al mercado el sorteo “Loterías Electrónicas en Cajeros Automáticos”, un innovador sorteo que consistía en elegir un número al azar en la pantalla de un cajero automático, con la posibilidad de obtener un premio que sería abonado a la cuenta del tarjetahabiente al instante.

Con este sorteo Lotería Nacional inició su incursión en el mercado de las nuevas tecnologías en sistemas de información, rompiendo su concepto tradicional de ventas de billetes de lotería impresos en papel y distribuidos mediante los leales “billeteros”.

Este trabajo proporciona el contexto general de la realización de este proyecto, desde su conceptualización hasta su implementación, enfatizando aquéllas actividades en las que como Actuarios podemos ofrecer soluciones de calidad en las diversas áreas en las que laboremos, ya sean de negocio, desarrollo, operación, etc.

Estructura del Trabajo

Los dos primeros capítulos de este trabajo (“Antecedentes” y “Objetivos de Marketing”) describen brevemente el surgimiento de las Loterías Electrónicas y los esfuerzos realizados para evaluar su factibilidad en el mercado.

Los siguientes tres (“Arquitectura de solución”, “Estudios estadísticos de Pseudo aleatoriedad”, y “Seguridad”) describen el diseño de la solución tecnológica que se implementó en el sorteo. Estos últimos capítulos abarcan las actividades en las cuales participé junto al equipo de trabajo de Lotería Nacional.

En cada capítulo la primera sección aborda conceptos teóricos que posteriormente son utilizados y dan una mayor claridad al contenido del trabajo.

Capítulo 1. Antecedentes

1. Introducción

Resulta sin duda interesante analizar el papel que ha desempeñado la suerte, los juegos de azar y la fe en ellos a través de la historia en diversas partes del mundo y la influencia que han tenido para la toma de decisiones. Es por ello que este trabajo empieza narrando algunas curiosidades al respecto.

Posteriormente se describe de una forma muy general el concepto y funcionalidad de las Loterías Electrónicas.

1.1 Antecedentes Históricos de las Loterías en el mundo

El origen del juego de la Lotería se da con los primeros pasos de la humanidad. Cuando por primera vez empezaron a reconocerse los derechos del individuo en la comunidad primitiva, el género humano debió sentirse atraído por ese juego que le permitía, valiéndose de varitas de distintas longitudes, o bien de piedras de diferente color, distribuirse de modo amistoso el trofeo de caza o el botín de guerra.

En las páginas de la Biblia encontramos algunas menciones al uso de las suertes, tanto para determinar la fortuna como para presagiar la desgracia.

En la India nos encontramos con una venerable forma de proceso legal cuya razón jurídica consistía en colocar en un recipiente imágenes de la inocencia y de la culpabilidad, obligando al acusado a sacar una de ellas, y el veredicto se dictaba según lo que aquél hubiese elegido.

En China y Japón se practicaba la adivinación (658 d. de J. C.). Los musulmanes también practicaban este arte valiéndose de nueces y güijas.

Un método romano para descubrir los acontecimientos era el empleo de *sortes*, que consistían en unas pequeñas varillas o fichas con inscripciones, las cuales iban atadas juntas, se sacaba una de ellas, se leía lo que llevaba inscrito y se interpretaba de manera que diese respuesta a la pregunta sometida por el que inquiría. Como vemos, esta idea llevaba en sí la semilla de Lotería, lo mismo que la palabra “sorteo” tiene su etimología en *sortes***.**

Nerón (37-68 d. de J. C.) en las fiestas que se celebraron por la eternidad del imperio, hizo echar al pueblo hasta mil billetes al día, unos daban un empleo y esclavos; otros, tierras y navíos.

Así como éstos, hay muchos rasgos sueltos en la historia, que nos muestran que el dejar la toma de una decisión a la suerte era un método utilizado tanto por hechiceros como por personajes con grados de autoridad en las respectivas comunidades.

1.2 Loterías Modernas

La Lotería Moderna es hija de los Países Bajos, se sabe que las *relaciones* (pequeños volantes precursores de los periódicos de hoy en día) de los años 1443-1449 muestran sorteos operados en varios puntos, tales como Gante, Utrecht, Audenarde, Brujas y L’Ecluse, y señalan el uso de la Lotería en los extensos territorios de los Duques de Borgoña.

En Brujas se realizaron Loterías el 24 de febrero de 1445 y el 24 de agosto de 1446 que juntas arrojaron una suma de 982 libras, 13 sueldos y 10 dineros flamencos de beneficio neto que ingresó a las arcas de la localidad.

Con los años fue aumentando el valor de los premios y a partir de 1490 se empezaron a pagar éstos con plata, en lugar de hacerlo con moneda.

Entre los años 1518 a 1529 se registraron veintiséis Loterías en el territorio que hoy comprende parte de los países de Holanda, Bélgica y Francia.

En Malinas en 1519 la población se lamentaba de los impuestos y no era aconsejable aumentar las cargas fiscales, así que había que incorporar una fórmula que estimulara la aportación económica de los ciudadanos hacia obras de beneficencia necesarias para la ciudad. Se decidió implementar una Lotería en gran escala y el resultado fue muy satisfactorio.

Por edicto el 2 de mayo de 1526 se prohíben todas las Loterías que no tenían licencia, bajo pena de confiscación de los premios y del dinero recibido, probablemente como un paso preliminar hacia la institución de una Lotería Estatal.

Hasta principios del siglo XX hubo en Alemania siete Loterías estatales: la Prusiana, la Sajona, la de Mecklemburgo-Schwerin, la de Brunswick, la de Hamburgo, la de Lubeck y la asociación de Loterías de Hesse-Turingia. La coexistencia de estas Loterías causó perjuicios a la de Prusia, por lo que tuvo que celebrar Tratados con los estados competidores regulando el que cada estado vendiera sus billetes sólo dentro de su territorio.

En 1938 se fundieron todas las Loterías de Alemania, cesando sus actividades al final de la guerra, en 1945.

En 1568 tuvo lugar una Gran Lotería en Inglaterra, para proveer fondos con destino al mejoramiento de los muelles.

Por lo que se refiere a la Lotería en los Estados Unidos de América, se sabe que la colonia de Virginia fue implantada, en su mayor parte, con ayuda de los sorteos organizados en 1612-1621, que se celebraron en Londres. Posteriormente las Loterías empezaron a generalizarse en los Estados Unidos a principios del siglo XVIII.

A partir de 1720, en Finlandia, las Loterías eran medios populares de hacer mejoras públicas. En Connecticut, en 1750, por medio de una Lotería se recaudaron los fondos para la edificación del Yale College.

Hemos desglosado los juegos de azar en diversos países y en diversas épocas pero no podría faltar, desde luego, algo sobre estos juegos en México, desde antes de la conquista.

1.3 Antecedentes de Loterías en México

En la América precolombina se conocían los juegos de azar, se tiene noticia de que entre los señores del imperio azteca, además del juego de pelota y del tiro al blanco con arco y flechas, se ejercitaban pasatiempos de juegos de azar, como el Patolli, que era análogo al de los dados, se utilizaban cuatro frijoles grandes, cada uno con un agujero en el centro, se les arrojaba sobre un petate donde estaba hecha una figura *como de aspa grande*, señala Fray Diego Durán en su Historia de las Indias.

Otro juego importante era el del Tololoque, que se jugaba con unos bodoquitos chicos de oro muy lisos. El juego consistía en tirar los bodoquitos hacia cinco líneas trazadas en el suelo, y que servían para calcular quien ganaba o perdía. Cuenta Bernal Días del Castillo que Moctezuma jugaba ese juego con Cortés.

Fueron los conquistadores españoles los que introdujeron el juego de naipes en América. Hernán Cortés era muy aficionado a los naipes y a los dados.

Cuando los españoles conquistaron la Gran Tenochtitlan, fue creciendo la inmoderada pasión por el juego, lo cual provoco problemas y riñas entre los habitantes durante 3 siglos de coloniaje. En este tiempo hubo muchos intentos fallidos por combatir el juego, los cuales terminaban empeorando la situación y volviendo a éste más clandestino. Finalmente se optó por no erradicar y prohibir las costumbres del juego sino más bien, darles orientación y control, y es así como Carlos III establece la Real Lotería en Nueva España.

Con todos estos antecedentes, podemos concluir que la Lotería Nacional para la Asistencia Pública –a la cual llamaremos LOTENAL en lo que resta de este trabajo-, máxima precursora de sorteos en nuestro país, no tiene su origen en el deseo de hacer el bien a los demás, o en ayudar en alguna forma a los necesitados, más bien fue creada con el objeto de evitar el juego sin control, y el de convertir en productiva esta afición tan arraigada de los conquistadores españoles, motivo de pleitos y hasta crímenes.

Posteriormente se emplearon las ganancias en muy diversas formas hasta llegar con el tiempo y su propia evolución a crear la imagen que hoy tiene la LOTENAL.

2. Necesidad de LOTENAL por implementar Loterías Electrónicas

Dejando atrás la historia y retomando el presente, indudablemente la Tecnología de la Información (TI) está cambiando la forma tradicional de hacer las cosas. Las personas que trabajan en gobierno, en empresas privadas, que dirigen personal o que trabajan como profesional en cualquier campo están utilizando la TI cotidianamente mediante el uso de Internet, las tarjetas de crédito, y el pago electrónico de la nómina por mencionar algunos ejemplos. Los avances actuales hacen posible capturar y utilizar la información en el momento que se genera, es decir, tener procesos en línea.

Este hecho no sólo ha cambiado la forma de hacer el trabajo y el lugar de trabajo sino que también ha tenido un gran impacto en la forma en la que las empresas compiten.

LOTENAL, hasta finales del 2003, había manejado un sistema tradicional de Loterías de “billetes físicos”, pero precisamente ante la gama de productos de la competencia existentes en el mercado y el rápido avance de la TI no podía quedarse atrás, tenía que ofrecer al público consumidor un producto que fuese original, atractivo y moderno, tanto para sus clientes como para las nuevas generaciones.

Es así como en LOTENAL surge la idea de desarrollar juegos interactivos en cajeros automáticos, que es de hecho, la primera loter en cajeros automáticos en el mundo.

3. Definición de Lotería Electrónica y solución propuesta

Las Loterías Electrónicas de LOTENAL proponen la realización de diversos sorteos mediante la emisión de billetes electrónicos ligados a una base de datos, con una mecánica de participación en medios electrónicos, distribuidos y comercializados a través de cajeros automáticos.

Los billetes electrónicos equivalen a los billetes físicos (billetes impresos), cada uno tiene un número con el cual participa en el sorteo de la misma forma como ocurre en la Lotería Tradicional (Zodiaco, Gordo de Navidad, etc.).

Los billetes electrónicos se almacenan en una Base de Datos Electrónica, a la cual llamamos Base de Datos de Premios. Por ejemplo, si LOTENAL autoriza para un sorteo electrónico una emisión de 500,000 billetes, significa almacenar un arreglo de números del 1 al 500,000 en la Base de Datos de Premios, de la misma forma en que el sorteo Zodiaco lanza a la venta 500,000 billetes impresos de Lotería, cada uno con su respectivo número de participación.

A pesar de que la idea fue concebida inicialmente pensando en los cajeros automáticos, LOTENAL buscó la forma de generalizar el concepto a una Lotería Electrónica, cuyo modelo de sorteos permitiera su comercialización a través de diversos puntos de venta, y que estuvieran respaldados por un sistema de administración apegado a la normatividad de LOTENAL.

LOTENAL en conjunto con HSBC (la institución bancaria que implementaría el sorteo), comenzaron el estudio de factibilidad del nuevo producto. En el siguiente capítulo abordaremos un resumen de este tema.

3.1 ¿Cómo colabora el Actuario en un proyecto de esta naturaleza?

El profesional de la actuaría es capaz de estudiar, plantear, formular y aplicar modelos de contenido matemático acerca de fenómenos que involucran riesgos, con el fin de proveer información para la planeación, la previsión y la toma de decisiones.

El actuario con su formación académica y conocimientos aplicados a las matemáticas, financieras, estadística, probabilidades y técnicas de muestreo podría perfectamente colaborar en actividades tales como:

- Estudio de factibilidad del producto
- Estimaciones de Ventas
- Análisis costo/beneficio

Sin embargo, mi participación en el proyecto se dio en la etapa de implementación tecnológica, en el área de la Dirección Informática.

3.2 Mi participación en el Proyecto

Cuando me incorporé al Proyecto de Loterías Electrónicas en LOTENAL, las áreas responsables ya habían realizado el plan de factibilidad y definido las reglas de negocio de proyecto, lo que faltaba era implementar la solución tecnológica.

Mi colaboración con el equipo de trabajo para alcanzar los objetivos del proyecto fue la siguiente:

1. Definición del Algoritmo de Aleatoriedad para la generación de billetes y asignación de premios.
2. Definición del Esquema de Seguridad utilizado en el modelo de datos (en conjunto con el área de Seguridad de la Institución).
3. Desarrollo e implementación del Producto.
4. Generación de documentación técnica.
5. Cierres contables al final del sorteo (basados en requerimientos específicos del área contable de la Institución).

El siguiente capítulo “Objetivos de Marketing” describe de forma general la estrategia mercadológica que siguió LOTENAL para el lanzamiento del sorteo. Se menciona en este trabajo para fines informativos, sin embargo yo no estuve involucrada en estas actividades.

A partir del capítulo 3 “Arquitectura de solución” los temas tratados corresponden a la solución tecnológica y herramientas utilizadas en la implementación del sorteo, y es precisamente en dichas actividades en las cuales participé junto al equipo de trabajo de LOTENAL.

3.3 Lotería Electrónica en Cajeros Automáticos

Vamos ahora a explicar un poco en qué consiste el sorteo, aunque en el capítulo 3 se verán más a detalle sus características técnicas.

3.3.1 Mecánica de participación

La mecánica de participación es la siguiente:

1. Participar en el cajero automático bancario con la tarjeta de débito respectiva.
2. Seleccionar la opción de “Sorteo Electrónico” en el menú principal de la pantalla.
3. Elegir el sorteo.
4. El sistema generará automáticamente 8 números aleatorios y los mostrará en la pantalla del cajero automático para que se seleccione el número de billete de su predilección.
5. Confirmar el número seleccionado.
6. Esperar 10 segundos a que el sistema verifique si el número seleccionado tiene premio.
7. Conocer el resultado por medio de la pantalla e imprimir el comprobante. En caso de ser ganador, la institución Bancaria depositará en su cuenta de manera instantánea el monto del premio menos los impuestos correspondientes

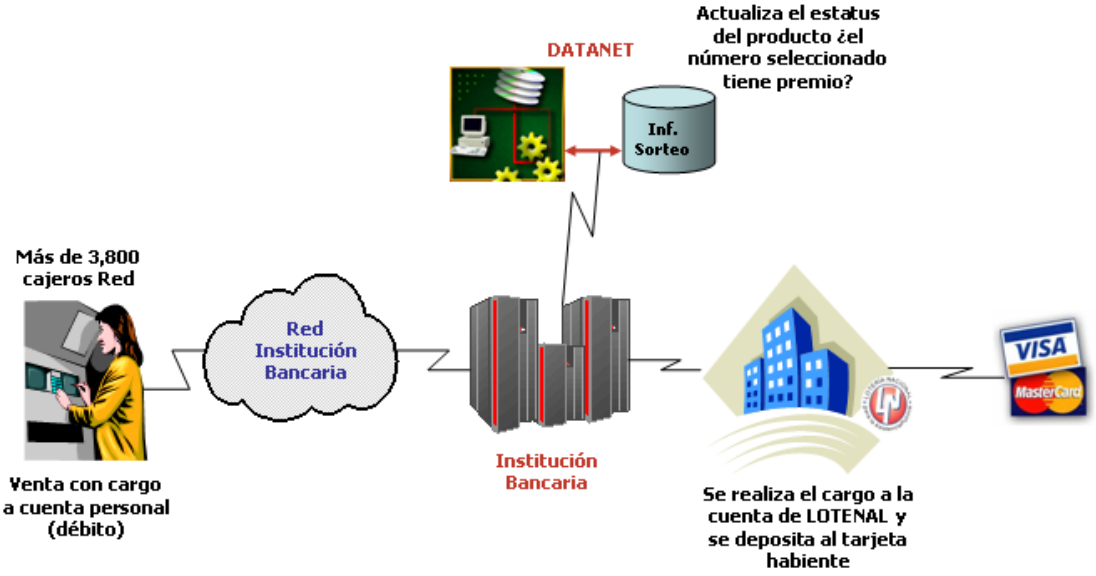


Figura 1.1 Modelo Operacional del sorteo Loterías Electrónicas

3.3.2 Aspectos Técnicos del Sorteo

Los procesos internos con los cuales opera el sorteo, y que se detallarán en la sección 3 de este trabajo, son los siguientes:

1. **Sembrado de Premios:** Este proceso consiste en generar una Base de Datos Electrónica, en la cual se encuentran los números de billetes participantes y su premio correspondiente. Este proceso es pseudo-aleatorio, está hecho en lenguaje de programación java y la cantidad de billetes participantes y de premios otorgados se basa en una Estructura de Premios oficial autorizada por el área de Mercadotecnia de LOTENAL. La información se registra en la Base de Datos, cifrada con un algoritmo 3DES[1].

2. **Generación de Números Participantes:** Cuando el usuario acepta participar en el sorteo, el sistema accede a la Base de Datos Electrónica y selecciona de manera aleatoria 8 números participantes, los cuales llamamos billetes electrónicos, estos se muestran en la pantalla del cajero automático para que el usuario seleccione el número de su agrado.

3. **Validación de Premios:** Cuando el usuario ha seleccionado el billete, el sistema verifica en la Base de Datos Electrónica el premio correspondiente, realiza una rutina para descifrar el

[1] En criptografía **Triple DES (3DES)** se llama al algoritmo que hace triple cifrado del **DES**. También es conocido como TDES o 3DES, fue desarrollado por IBM en 1978.

valor del premio, recordemos que este se encuentra en la Base de Datos cifrado con un algoritmo 3DES, si tiene asociado un premio se calculan los impuestos correspondientes y se devuelve esta información cifrada con un algoritmo DES[2]. El resultado de la validación del premio se muestra en la pantalla del cajero automático, indicando si es el caso, el valor del premio y los impuestos retenidos. El premio se abona inmediatamente en la cuenta del tarjetahabiente y lo puede corroborar en ese mismo instante en el cajero automático.

3.3.3 Actores Involucrados

En este sorteo están involucrados LOTENAL y la Institución Bancaria que va a vender el producto, Además existe otra figura cuya responsabilidad es proveer la arquitectura tecnológica que comunica a LOTENAL con el Banco, a esa figura la llamaremos "Distribuidor".

El modelo operacional permite ampliar el concepto de los sorteos electrónicos y no limitarlos solamente a cajeros automáticos, podemos pensar en cualquier punto de venta electrónico como internet, cajas registradoras, teléfonos celulares, etc., y un Distribuidor será cualquier organización que pueda certificar ante LOTENAL que cuenta con la infraestructura de comunicación necesaria entre el Centro de Datos y los puntos de venta.

Los requisitos que debe cubrir una organización para ser Distribuidor son:

1. Estar certificados en ISO 9000[3].
2. Aplicar para ser distribuidores de LOTENAL (llenar solicitud).
3. Celebrar el contrato de comisión mercantil con una comisión de 10% según la Ley Orgánica de la Entidad.
4. Ser autorizado por el Comité.

En las Loterías Electrónicas en cajeros automáticos, el Distribuidor autorizado fue Datanet de México.

3.3.4 Beneficios para LOTENAL

Este sorteo permitiría a LOTENAL:

1. Proyectar una imagen de modernidad a través de tecnología, dejando de lado su imagen tradicional (venta de billetes físicos).
2. Proyectar una imagen de innovación al buscar nuevas formas de acercamiento con el consumidor. A nadie se le había ocurrido una idea de este tipo (idea muy creativa).
3. Proyectar una imagen de seriedad absoluta al estar relacionada con una institución bancaria.
4. Confiabilidad y honestidad al tratarse de un juego electrónico.
5. Idea de placer instantáneo debido a que el premio se obtiene de manera inmediata por medio de la cuenta bancaria.
6. Practicidad en el acceso y en el juego mismo.
7. Atraer nuevos perfiles de usuario en rangos de edad, nivel socioeconómico e incluso usuarios con un estilo de vida y hábitos de consumo diferentes.

3.3.5 Beneficios para el Banco

Este sorteo permitiría al Banco:

1. Adquirir una imagen de diversión para el banco. En general, las instituciones bancarias son aburridas y normalmente producen más dolor que placer.
2. Adquirir una imagen de innovación, ya que ningún otro banco tiene este servicio.

---

[2] **Data Encryption Standard (DES)** es un algoritmo de cifrado, es decir, un método para cifrar información, escogido como FIPS en los Estados Unidos en 1976, y cuyo uso se ha propagado ampliamente por todo el mundo.

[3] Conjunto de normas sobre calidad y gestión continua de calidad, establecidas por la Organización Internacional de Normalización (ISO)

3. Proyectar a sus clientes que cuenta con tecnología de punta ofreciendo sorteos instantáneos que responden y hacen operaciones en segundos.
4. Implementar moda, sobre todo con el paso del tiempo y cuando el consumidor entienda de manera clara los beneficios y mecánica de los juegos.
5. Ser una institución facilitadora de ganar dinero al brindar la oportunidad de practicar juegos de azar en sus cajeros automáticos.
6. Ganar lealtad y agradecimiento si el consumidor gana premios.
7. Diversificar servicios.
8. Mayor número de visitas de sus clientes al cajero, lugar donde se pueden promocionar otros productos bancarios.

Capítulo 2. Objetivos de Marketing

1. Introducción

Para establecer la mecánica de los sorteos electrónicos de LOTENAL, así como la estrategia de publicidad e imagen del producto, se realizó un estudio de mercado con el fin de captar las necesidades, deseos, posibilidades económicas y aceptación del público, y de esta forma garantizar el éxito del proyecto con un mayor grado de certeza.

En este capítulo se describen algunos conceptos generales de mercadotecnia y posteriormente el material cualitativo y cuantitativo recopilado por LOTENAL para la realización del estudio de mercado. Los conceptos teóricos ayudarán a comprender mejor éstas técnicas y el porqué de su elección entre la variedad de métodos y estrategias mercadológicas existentes.

1.1 Investigación de Mercado

La investigación de mercado es una técnica que permite recopilar datos, de cualquier aspecto que se desee conocer para, posteriormente, interpretarlos y hacer uso de ellos. Sirven al comerciante o empresario para realizar una adecuada toma de decisiones y para lograr la satisfacción de sus clientes.

La definición oficial, de acuerdo con la *American Marketing Association* es la siguiente:

"La investigación de mercados es la función que vincula al consumidor, al cliente y al público con el mercadólogo a través de la información – información que se utiliza para identificar y definir oportunidades y problemas de mercadotecnia; generar, afinar y evaluar las acciones de mercadotecnia; monitorear el desempeño de la mercadotecnia; y mejorar la comprensión de la mercadotecnia como un proceso. La investigación de mercados especifica la información requerida para atender estos aspectos, diseña el método para recabar la información, administra e implementa el proceso de recolección de datos, analiza y comunica los hallazgos y sus implicaciones."

1.2 El Mercado

Un mercado está constituido por personas que tienen necesidades específicas no cubiertas y que, por tal motivo, están dispuestas a adquirir bienes y/o servicios que los satisfagan y que cubran aspectos tales como: calidad, variedad, atención, precio adecuado, entre otros.

1.3 Tipos de Mercado

Se puede hablar de mercados reales y mercados potenciales. El primero se refiere a las personas que, normalmente, adquieren el producto; y, el segundo, a todos los que podrían comprarlo.

1.4 Segmentación de Mercados

La segmentación de mercados es un proceso mediante el cual se identifica o se toma un grupo de compradores con características similares, es decir, se divide el mercado en varios segmentos, de acuerdo con los diferentes deseos de compra y requerimientos de los clientes.

1.5 El Producto

Un producto es todo aquello que puede ofrecerse a un mercado para su uso o consumo y que, además, puede satisfacer un deseo o necesidad. Abarca objetos físicos, servicios, personas, sitios, organizaciones e ideas.

1.6 Estrategias de Mercadotecnia

Comprenden la selección y el análisis del mercado, es decir, la elección y el estudio del grupo de personas a las que se desea llegar, así como la creación y permanencia de la mezcla de

mercadotecnia que las satisfaga. En síntesis, la estrategia de mercadotecnia es un tipo de estrategia con el que cada unidad de negocios espera lograr sus objetivos de mercadotecnia mediante:

1. La selección del mercado meta al que desea llegar.
2. La definición del posicionamiento que intentará conseguir en la mente de los clientes meta.
3. La elección de la combinación o mezcla de mercadotecnia con el que pretenderá satisfacer las necesidades o deseos del mercado meta.
4. La determinación de los niveles de gastos en mercadotecnia.

1.7 Elementos de la Estrategia de Mercadotecnia

Analizando la definición anterior, se pueden visualizar cuatro elementos clave que componen la estructura básica de la estrategia de mercadotecnia:

1. El mercado meta: Se refiere a un grupo bastante homogéneo de clientes a quienes una compañía determinada quiere atraer.
2. El posicionamiento: Consiste en hacer que un producto ocupe un lugar claro, distintivo y deseable, en relación con los productos de la competencia, en las mentes de los consumidores meta.
3. La combinación de mercadotecnia: Son las variables (producto, plaza, precio y promoción) que una empresa combina y controla para satisfacer ese mercado.
4. La determinación de los niveles de gastos en mercadotecnia: Incluye un presupuesto general que da una idea global acerca de cuánto dinero se necesitará para implementar el plan de mercadotecnia en su totalidad.

1.8 Métodos de recolección de datos

El diseñador de la investigación tiene una amplia variedad de métodos a considerar para la recolección de datos, ya sea de manera individual o combinados. Estos métodos se pueden agrupar primero con base en si usan fuentes secundarias o primarias de datos.

- **Datos Secundarios:** Son aquellos que fueron recolectados en el pasado por personas o agencias respondiendo a un propósito determinado que en general, no corresponde al propósito del problema del presente, pero que sin duda ofrecen al investigador ahorro en costos y tiempo, además de que ayudan a definir la población, la muestra en la recolección de datos primarios y muchas veces, el problema y su posible solución.

- **Datos Primarios:** Son aquellos que se recolectan especialmente para un objetivo específico de investigación. Los métodos de recolección de estos datos van desde la investigación cualitativa, encuestas y hasta experimentos. La investigación cualitativa se usa para obtener mayor conocimiento sobre los beneficios que buscan los clientes y las fuentes de insatisfacción con los productos existentes.

Estos métodos se describen a mayor detalle en la siguiente tabla:

Método de Recolección de datos	Categoría de la Investigación Exploratoria	Descriptiva	Causal
Fuentes Secundarias			
• Sistemas de Información	a	b	
• Bancos de datos de otras organizaciones	a	b	
• Servicios sindicados	a	b	b
Fuentes Primarias			
• Investigación cualitativa	a	b	
• Encuestas	b	a	b
• Experimentos		b	a
a = Método muy apropiado	**b = Método algo apropiado**		

Tabla 2.1 Relación entre el Método de recolección de datos y la categoría de la Investigación

1.9 Investigación cualitativa

El propósito de la investigación cualitativa es descubrir lo que hay en la mente de un consumidor. Se realiza a fin de tener acceso a la perspectiva de la persona y, a la vez, formarse una idea aproximada de la misma. Los datos cualitativos se recopilan para conocer más acerca de cosas que no se pueden observar y medir directamente. Los sentimientos, pensamientos, intenciones y comportamientos que tuvieron lugar en el pasado son algunos ejemplos de aquellas cosas que sólo se pueden obtener mediante métodos de recolección de datos cualitativos.

En ocasiones tal vez no sea posible o deseable obtener información de los entrevistados empleando métodos totalmente estructurados o formales, ya que las personas no siempre están dispuestas a responder preguntas cuando se les confronta directamente, sobre todo aquellas que perciben como una invasión de su privacidad, que piensan que los puede avergonzar o tener un impacto en su ego, este tipo de preguntas simplemente no serán contestadas. En estos casos se utilizan los métodos de recolección de datos cualitativos.

Se ha demostrado que la información de este tipo puede obtenerse mejor a través de métodos cualitativos, como discusiones de grupos de enfoque o técnicas de proyección, que mediante un método formal de encuesta estructurada de recolección de datos.

1.10 Grupos de Enfoque (Focus - Groups)

Una discusión de un grupo de enfoque es el proceso para obtener posibles ideas o soluciones a un problema de mercadotecnia discutiéndolo con un grupo de entrevistados. El énfasis de éste método está en los resultados de la interacción del grupo cuando se concentra en una serie de temas que el líder de la discusión presenta. A cada participante de un grupo de cinco a nueve o más personas se le motiva para que exprese sus puntos de vista sobre cada tema, y luego que amplíe o responda frente a los puntos de vista de los demás participantes. En las discusiones de grupos de enfoque el moderador desempeña un papel más pasivo que en el caso de un entrevistador.

La discusión de un grupo de enfoque ofrece a los participantes mayor estímulo que una entrevista, supuestamente esto hace que aumente la posibilidad de nuevas ideas y comentarios significativos[4]. Entre otras ventajas, se afirma que las discusiones a menudo generan más espontaneidad y franqueza que lo que puede esperarse en una entrevista.

[4] Martín Lautman, “Focus Groups” Theory and Method”, Advances in Consumer Research 9, p. 54.

Ahora que conocemos estos conceptos básicos, podemos utilizarlos para explicar un poco sobre las estrategias de mercadotecnia utilizadas en las Loterías Electrónicas.

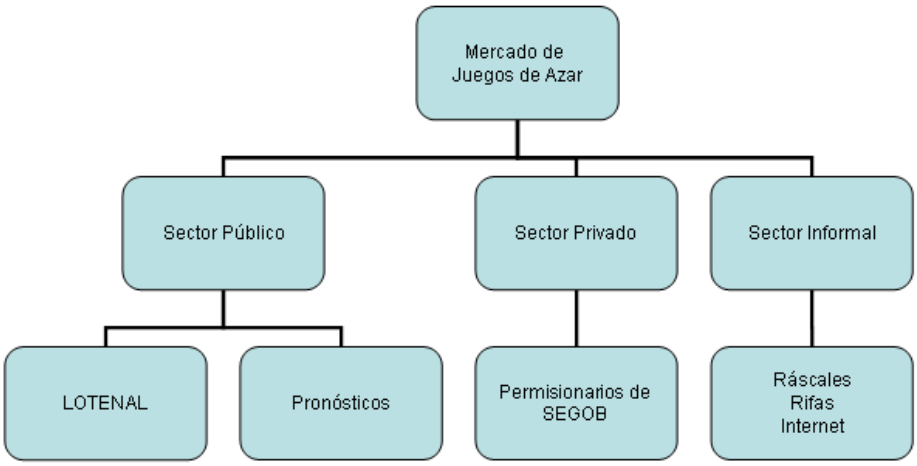
2. Estudio de Mercado de Loterías Electrónicas

2.1 Recolección de Datos Primarios

El primer paso fue la recopilación de todos aquellos datos que pudieran servir para definir el mercado meta del producto. La base inicial fue realizar una búsqueda de datos primarios que aportaran valor a la investigación, recurriendo a diversas fuentes de información.

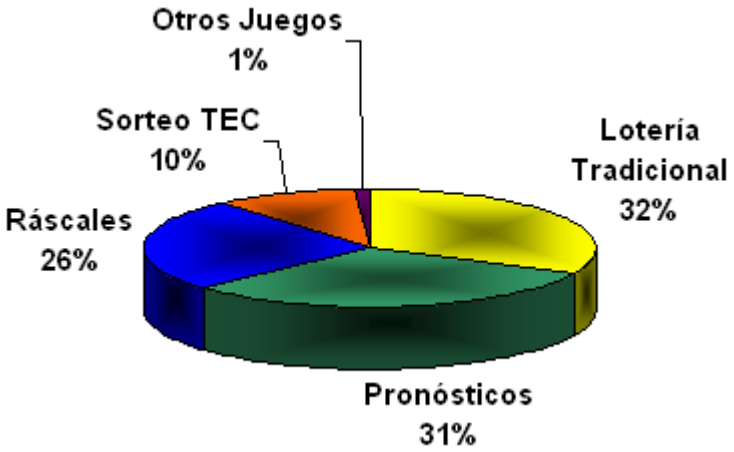
Algunos de los datos primarios recolectados se muestran en las siguientes gráficas:

1. Mercado de Juegos de Azar (Fuente: Acervo LOTENAL 2002)



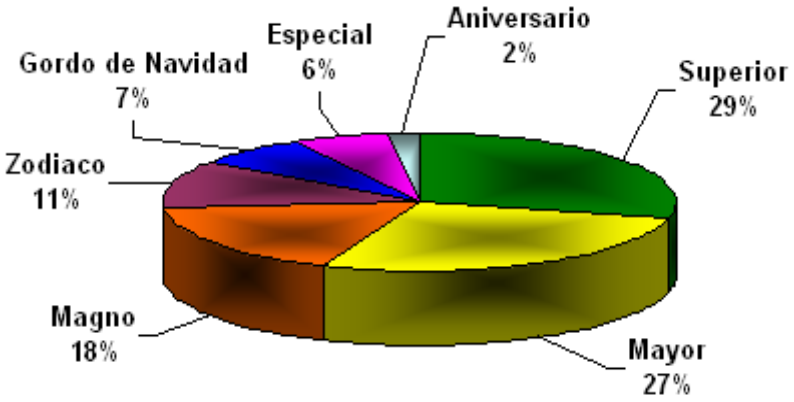
Nota: Los permisionarios condicionados regalan sus boletos de participación como promoción o los otorgan en función de las compras que realizan sus clientes, son una especie de bonificación por volumen

2. Simulación del Mercado: El consumidor mexicano dedica un 0.7% del PIB a jugar Lotería (Fuente: INEGI 1999)



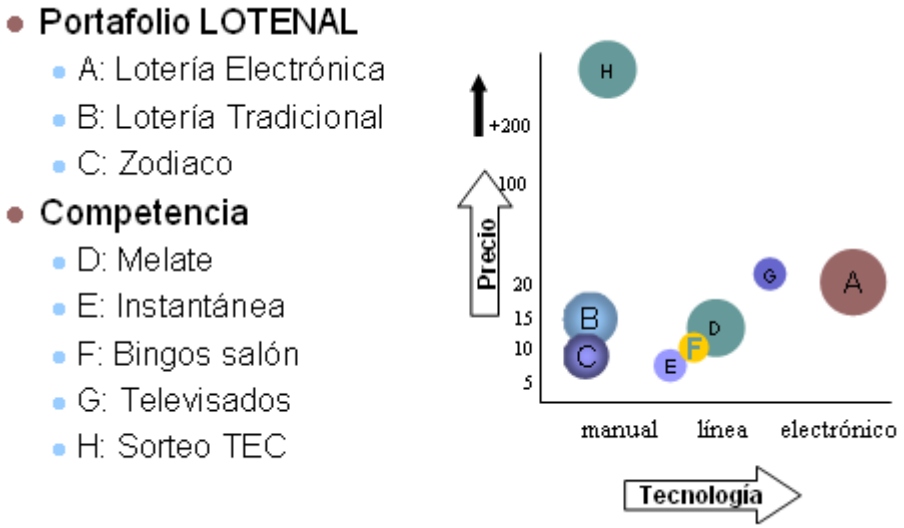
Gráfica 2.1 Productos de Juegos de Azar en el mercado

3. Portafolios de Productos de LOTENAL: Pertenecen a una línea de productos conocida como “sorteos tradicionales”. (Fuente: Informe Anual de Ventas 2001, Dirección de Mercadotecnia)



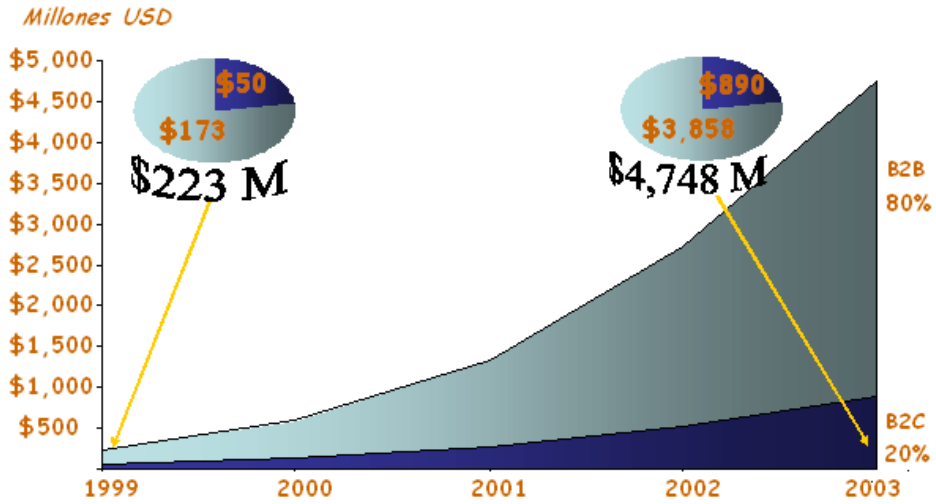
Gráfica 2.2 Productos de Lotería Nacional en el mercado

4. Precios de productos en el Mercado de los Juegos de azar 2001, incluyendo Lotería Electrónica y su precio tentativo. (Fuente: Puntos de Venta y medios de comunicación)



Gráfica 2.3 Precios y tendencia del mercado de juegos de azar

5. Estadísticas de Proyección de Ventas por concepto de Comercio Electrónico en México, 1999-2003 (Fuente: Select IDC[5], México)



Gráfica 2.4 Estadísticas de Proyección de Ventas

2.2 Mercado Meta

Dado que el medio de comercialización de los sorteos electrónicos sería inicialmente cajeros automáticos, el mercado meta hacia el cual se enfocaría el producto serían aquellos usuarios tarjetahabientes de la institución bancaria (tarjeta de débito).

De acuerdo a estadísticas del banco HSBC (2002) sobre el sector de la población que utiliza cajeros automáticos para retirar efectivo tenemos los siguientes resultados:

- 64% son hombres y 36% mujeres.
- Aquellos con edad de 19 a 35 años constituyen el 52%, y de 36 a 45 años el 31%
- En promedio, este sector corresponde al nivel socioeconómico "C" típico. (Ver Tabla de Grupos de Nivel Socioeconómico)

Grupo	Ingreso	Educación	Ocupación
A	El más alto	Posgrado o extranjero	Dueño o socio
B	Alto	Posgrado	Director
C	Medio	Profesional	Gerencia
D	Medio Bajo	Pasante o preparatoria	Empleado
E	Bajo	Secundaria o menos	Empleado o subempleado

Tabla 2.1 Tabla de Grupos de Nivel Socioeconómico (NSE)

También se concluyó que en este sector pueden o no ser jugadores de lotería u otros juegos de azar, sin embargo, es gente que tiene curiosidad por probar su suerte y puede jugar si es que el costo no es muy alto y si no se le complica en cuanto a mecánica, tiempo o seguridad personal.

2.3 Imagen del Sorteo Electrónico

Al mismo tiempo que el área de Mercadotecnia de LOTENAL definía la estrategia a utilizar, el área de Nuevos Productos trabajaba en el diseño y la imagen del sorteo. El resultado final fue el siguiente:

[5] IDC es el líder global de inteligencia de mercados y firma de consultoría en las industrias de Tecnologías de la Información (TI) y Telecomunicaciones. La firma analiza y predice tendencias tecnológicas con el fin de que sus clientes puedan tomar decisiones estratégicas de compra en TI, así como también de tácticas de negocios.

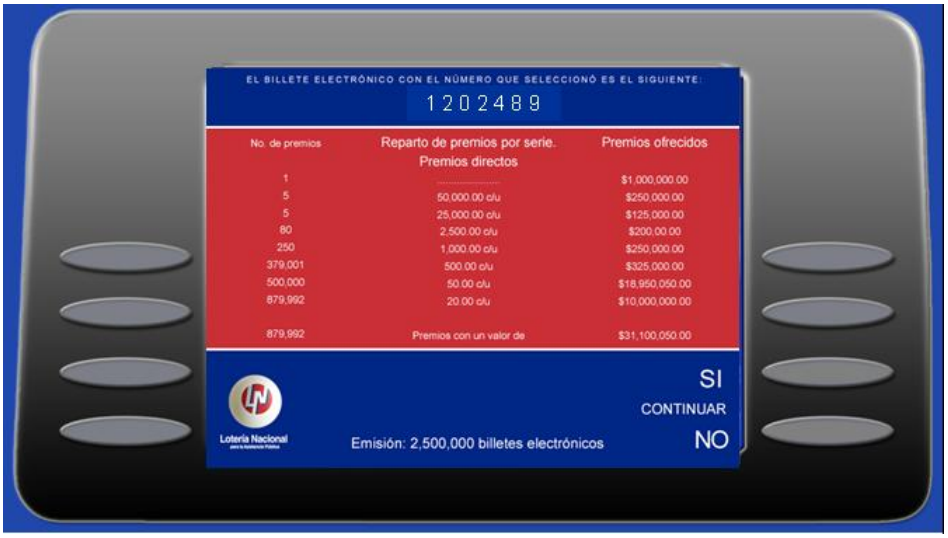
1. Pantalla inicial del Cajero Automático

2. Pantalla de participación en el sorteo

3. Pantalla con la imagen de los sorteos

4. Pantalla de selección de número participante (billete electrónico)

5. Pantalla de confirmación (muestra la estructura de premios autorizada por LOTENAL).



La estructura de premios se refiere a la distribución de los premios en el universo total de billetes electrónicos de la emisión. Debe ser avalada por las áreas de Mercadotecnia y Nuevos Productos de LOTENAL. La estructura de premios puede variar de un sorteo a otro. La siguiente tabla muestra la estructura de premios oficial de un sorteo electrónico con un periodo de vida en el mercado de 3 a 4 meses aproximadamente.

No. PREMIOS	REPARTO DE PREMIOS			MONTO TOTAL DE PREMIOS OFRECIDOS
	PREMIOS DIRECTOS			
1	PREMIO DE			$1,000,000.^{00}
5	PREMIOS DE	$50, 000.^{00}	CADA UNO	$250,000.^{00}
5	PREMIOS DE	$25,000.^{00}	CADA UNO	$125, 000.^{00}
80	PREMIOS DE	$2,500.^{00}	CADA UNO	$200, 000.^{00}
250	PREMIOS DE	$1,000.^{00}	CADA UNO	$250, 000.^{00}
650	PREMIOS DE	$500.^{00}	CADA UNO	$325, 000.^{00}
379,001	PREMIOS DE	$50.^{00}	CADA UNO	$18,950,050.^{00}
500,000	PREMIOS DE	$20.^{00}	CADA UNO	$10,000, 000.^{00}
879,992	**PREMIOS CON UN VALOR DE**			**$31,100,050.^{00}**

Tabla 2.2 Estructura de Premios

La estructura nos dice que hay 1 premio de $1,000,000.^{00}, 5 premios de $50,000.^{00} cada uno, los cuales suman un total de $250,000.^{00} pesos; y así sucesivamente.

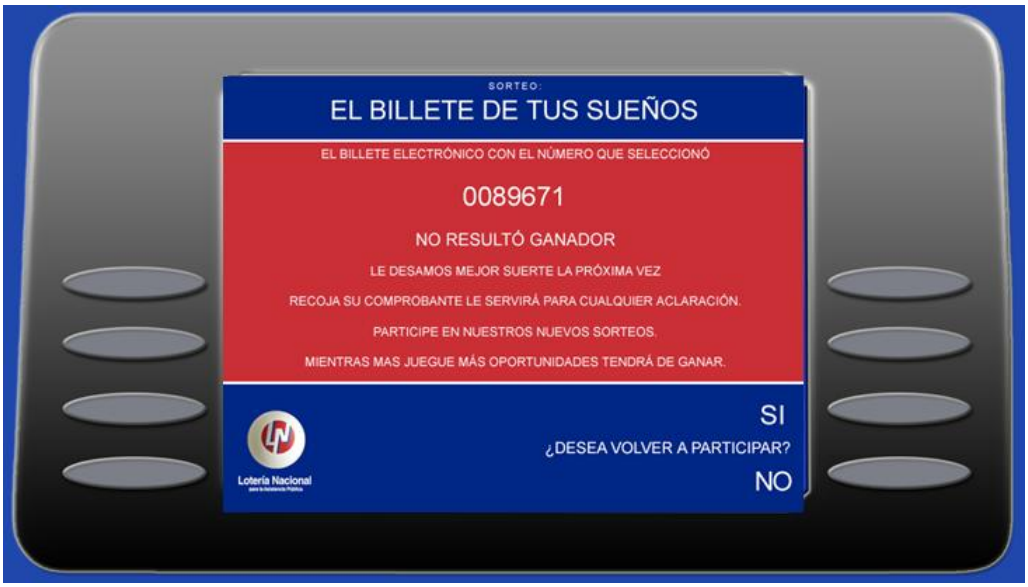
Características de la Estructura de Premios

- Premio principal: $1,000,000.^{00} (un millón de pesos menos impuestos)
- Tamaño de la Emisión: 2,500,000 billetes electrónicos
- Valor de la Emisión: $50,000,000.^{00} (cincuenta millones de pesos) [6]
- Precio del billete electrónico: $20.^{00} (veinte pesos)
- Repartible: 62.20% (sesenta y dos punto veinte por ciento)[7]
- Probabilidad de ganar un premio: 2.8% (dos punto ocho por ciento)[8]

6. Pantalla de espera de resultados (¡¡segundos de emoción!!)

[6] Calculada multiplicando el valor del billete ($20.^{00}) por el total de billetes de la emisión (2,500.000)
[7] Equivale al porcentaje del monto total de premios ofrecidos ($31,100,050.^{00}) con relación al valor de la emisión ($50,000,000.^{00})
[8] Calculada dividiendo el total de billetes de la emisión (2,500,000) entre el total de premios repartidos (879992)

7. Pantalla de resultados. En caso de ser un billete ganador, se mostraría el monto total del premio, los impuestos retenidos, y el monto neto del premio, el cual sería abonado inmediatamente a la cuenta bancaria del participante.



8. Recibo de participación del cliente. El cajero automático expediría el recibo comprobante de participación del cliente.

```
          LOGO DE LA
     INSTITUCION BANCARIA


11/12/2002        10:25        DBR001

       P.INDS. EXPORTEC 1
       TOLUCA, EDO. DE MEXI 001

TARJETA: 4900                      (13)
FOLIO: 0010

 LOTERÍA NACIONAL PARA L ASISTENCIA
PÚBLICA                 SORTEO: 99999

DISP PARA LOTERÍA ELECTRÓNICA
SORTEO: "EL BILLETE DE TUS SUEÑOS"

NUMERO SELECCIONADO:          1894899
VALOR BILLETE ELECTRÓNICO:      $20.00
MONTO PREMIO:            $1,000,000.00
MONTO IMPUESTO:             $70,000.00
MONTO NETO DEL PREMIO:     $930,000.00
    EL MONTO NETO DEL PREMIO FUE
         ABONADO A SU CUENTA
    VIGENCIA SORTEO: DD/MM/YYYY
CONSERVE SU RECIBO COMO COMPROBANTE
PARA CUALQUIER ACLARACIÓN SOBRE LA
TRANSACCIÓN ACUDE A TU SUCURSAL
BANCARIA.                          (33)
```

2.4 Estrategia de Mercadotecnia a utilizar en Loterías Electrónicas

Como las Loterías Electrónicas están enfocadas hacia un segmento particular de la población, las características del producto, campañas publicitarias e introducción al mercado estarían diseñadas pensando exclusivamente en dicho segmento. A esto se le conoce como "Mercadotecnia de selección de Mercado".

Debido a las ventajas que ofrecía utilizar los métodos cualitativos en la investigación y con la finalidad de detectar el agrado, interés y aceptación del sorteo en el consumidor, LOTENAL solicitó a Estudios Psico Industriales la realización de un estudio cualitativo de mercado, el cual tuvo como objetivos de investigación los siguientes temas:

- Sugerencias para el diseño, parte gráfica y mecánica de los sorteos propuestos.
- Sugerencias del valor/precio de los diferentes sorteos.
- Grado de satisfacción/identificación.
- Identificar los atributos/beneficios percibidos.
- Interés generado para participar en los sorteos.
- Reacciones espontáneas: afectivas/racionales.
- Nivel de impacto/aceptación.
- Obtener sugerencias de la secuencia de introducción de los distintos sorteos dados los posibles niveles de cansancio de los mismos.
- Obtener sugerencias en turno a nuevos sorteos.
- Determinar la estrategia de comunicación de estos sorteos.
- Establecer, si es que existen, nuevas motivaciones y frenos al uso más frecuente de los sorteos
- Determinar específicamente cuáles serían los beneficios de imagen para LOTENAL al realizar estos sorteos.

Para tal efecto se realizaron 3 sesiones de discusiones de grupos de enfoque, en las cuales se mostró la imagen y el concepto del producto resultado del trabajo de las áreas de Mercadotecnia y Nuevos Productos de LOTENAL.

2.5 Estudio Cualitativo de Pruebas de Concepto (focus groups) realizado por Estudios Psico Industriales (2002)

2.5.1 Ejemplos de grupos evaluados

Grupos	Características	NSE
1	Sesión mixta. Edad 20 – 29, todos solteros. 100% de los participantes fueron tarjeta habientes de DÉBITO HSBC, usuarios de cajeros automáticos y utilizarlos como mínimo dos veces por mes.	C Típico
1	Mujeres. Edad 30 – 42, todas casadas. 100% de las participantes fueron tarjeta habientes de DÉBITO HSBC, usuarias de cajeros automáticos y utilizarlos como mínimo dos veces por mes.	C Típico
1	Hombres. Edad 30 – 42, todos casados. 100% de los participantes fueron tarjeta habientes de DEBITO HSBC, usuarios de cajeros automáticos y utilizarlos como mínimo dos veces por mes.	C Típico

2.5.2 Tópicos de las sesiones

1. Breve exploración sobre los Juegos de Azar
    - El gusto por el juego
    - Las apuestas montos y probabilidades
    - Juegos preferidos

2. Percepciones sobre el uso de ATMs
    - Los servicios bancarios
    - La accesibilidad de los ATMs (frecuencia)
    - Los cajeros HSBC
    - La venta de otros servicios y productos.

3. Las Apuestas en ATMs
    - Pertinencia de juegos en ATMs
    - El tiempo para apostar
    - Características que deben de tener los juegos en ATMs

4. Exploración de preferencias sobre los juegos propuestos
    - El Billete de Tus Sueños
    - Sueño de Navidad

5. Costo de las Apuestas
    - Precios de cada jugada
    - Premios: Número y Montos
    - Jugadas Gratis
    - Pago instantáneo

6. Preferencias Generales
    - Cambio de Juegos
    - Otras opciones de juegos de azar (Pronósticos, Lotería).

2.6 Resultado del estudio cualitativo

2.6.1 Aceptación del Sorteo

- Los entrevistados se entusiasmaron con el nuevo concepto de sorteo electrónico y todos afirmaron que participarían en los cajeros automáticos bancarios. La imagen de LOTENAL era un gran aval de confianza, transparencia y seriedad al sorteo.
- El participar, dentro de las circunstancias inherentes a un cajero automático, se consideró como una tentación irresistible. No se registraron objeciones importantes sobre la conveniencia de que estos sorteos se realizan a través de cajeros automáticos. De cualquier manera se consideró que habría unos cajeros más idóneos que otros. La mayoría pensó que aquellos que estuvieran en centros comerciales serían los más apropiados.
- La reacción más importante hacia los sorteos electrónicos fue de curiosidad e interés, aun antes de conocer su mecánica de juego y la relación precio / premio.

2.6.2 Ventajas encontradas en este nuevo concepto de sorteos

- La facilidad de las instrucciones del sorteo, es decir su mecánica fue fácil y sencilla.
- Disponer del premio de inmediato fue un atributo absolutamente básico, que impactó muchísimo.
- La relación de probabilidades de ganar de 1 en 2.8 fue entendida con facilidad. Para ellos esto quiso decir “de cada casi tres jugadas tengo un chance de ganar”.

- La entrega del comprobante de la “transacción” realizada le otorgó mucha formalidad y credibilidad al juego.
- El precio de $20.00 fue considerado muy razonable y cómodo
- El promedio en el que los participantes acudían al cajero automático fue entre 2 y 3 veces por quincena. De todas estas ocasiones, ellos aseguraron participar en más de la mitad de ellas.

2.6.3 Desventajas y dificultades encontradas

- Un posible problema fue el de que muchos consideraron que la ley de probabilidades era “constante”, es decir, que siempre de cada tres jugadas esperarían un premio.
- Una pregunta que varias veces surgió fue la de poder escoger otros números diferentes a los arrojados por el sistema, ya que “cada quien tiene sus números”, y en el fondo hay unos números que se sienten “más” atractivos que otros. En caso de que no puedan escoger otros números, aparentemente este factor sería una pequeña desventaja del sorteo. Sin embargo, en la práctica, la mayoría de los participantes optarían por seleccionar uno de los ocho números que aparecen en pantalla.

2.6.4 Recomendaciones

- Se encontró un gran entusiasmo por el sorteo electrónico evaluado, y por tanto se recomendó su lanzamiento.
- Especificar que los $20.^{00} son con el precio total del billete, sin impuestos adicionales.
- Renovar los temas del sorteo de ser posible cada dos meses.

Capítulo 3. Arquitectura de solución

1. Introducción

El Modelo de Loterías Electrónicas desarrollado por LOTENAL está basado en la arquitectura Cliente/Servidor.

Este capítulo comienza describiendo algunos conceptos teóricos que posteriormente se utilizan en la explicación técnica de la arquitectura implementada en el proyecto.

1.1 Cliente

El Cliente es una aplicación informática que se utiliza para acceder a los servicios que ofrece un Servidor, normalmente a través de una red de telecomunicaciones.

El término se usó inicialmente para las llamadas "terminales tontas", dispositivos que no eran capaces de ejecutar programas por sí mismos, pero podían conectarse a una computadora central y dejar que ésta realizara todas las operaciones requeridas, mostrando luego los resultados al usuario. Se utilizaban sobre todo porque su costo en esos momentos era mucho menor que el de una computadora.

Actualmente se suele utilizar el término para referirse a aplicaciones que requieren específicamente una conexión a otro programa, al que se denomina "Servidor" y que suele estar en otra máquina.

1.2 Servidor

Es la máquina desde la que se suministran servicios y que está a la espera del requerimiento del cliente. Una vez hecho el requerimiento, busca la información solicitada y le envía la respuesta al cliente, incluso puede responder a varias solicitudes de servicios a la vez.

1.3 Arquitectura Cliente/Servidor

Después de revisar las definiciones anteriores resulta natural entender que esta arquitectura consiste básicamente en un Cliente que realiza peticiones a otro programa, el Servidor, que le da respuesta.

Entre las características fundamentales de esta arquitectura encontramos que tanto el Cliente como el Servidor pueden realizar tareas ya sea en forma conjunta o separada, ya que el Cliente también tiene sus propias aplicaciones, archivos y bases de datos, además, pueden estar en la misma plataforma o en plataformas diferentes.

Por otra parte, el Servidor puede brindar varios servicios a la vez, tanto al mismo Cliente como a clientes múltiples.

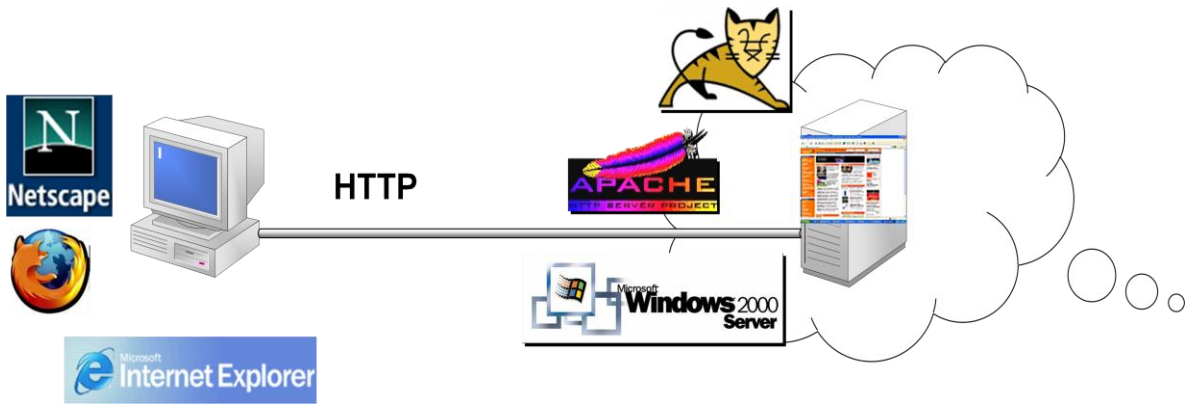


Figura 3.1 Arquitectura Cliente/Servidor

2. Definición de Algoritmos utilizados en Loterías Electrónicas

Cuando el usuario decide participar en Lotería Electrónica y selecciona en el cajero la opción de jugar, se ejecuta un proceso para mostrar en pantalla ocho números aleatorios de los cuales el usuario debe elegir aquel que sea de su agrado. Una vez elegido el número, se ejecuta otro proceso que valida si existe un premio asignado al número de participación seleccionado, y se muestra en pantalla el resultado.

Los Algoritmos de Loterías Electrónicas son los programas hechos en java J2SE 1.3[9] que implementan los procesos necesarios para realizar la logística de participación, además de la creación, monitoreo, cierre y verificación del sorteo, porque, aunque la cara ante el cliente pareciera ser solamente la mecánica del juego, se requiere de un proceso previo de creación y autorización, y un proceso posterior de cierre y validación del sorteo, basados en procedimientos institucionales apegados a la normatividad de la LOTENAL.

Los Algoritmos de Loterías Electrónicas encapsulan toda esta funcionalidad en un software llamado "Loterías Electrónicas", el cual está basado en la arquitectura Cliente/Servidor y registrado como propiedad intelectual de la LOTENAL.

En el siguiente cuadro se muestran los principales procesos incluidos en las Loterías Electrónicas:

Algoritmo de Sembrado de Premios	1. Se construye una colección de números (billetes electrónicos) en base a las emisiones de billetes autorizadas por LOTENAL (universo de números a sortear). Por ejemplo, una emisión de 1,000,000 números contendrá billetes del 1 al 1,000,000. 2. Aplicando funciones pseudo-aleatorias propias del lenguaje de implementación se "revuelven" los números o billetes participantes. esto significa que después de aplicar el proceso de asignación aleatoria el número o billete 1 no necesariamente se encontrará en la posición 1 de la colección. 3. Se construye una colección con los premios a sortear de acuerdo con las estructuras de premios y emisiones autorizadas por LOTENAL, esto significa que tendremos una colección del tamaño de la emisión de billetes electrónicos en la cual cada entrada corresponderá a un premio autorizado o "cero" cuando no haya premio. 4. Aplicando funciones pseudos-aleatorias propias del lenguaje de implementación se realiza una distribución al azar de dichos premios (se "revuelven"). 5. Se realiza el algoritmo de asignación entre la colección de billetes electrónicos y la colección de premios, es decir, a cada número participante se le asigna un premio de forma aleatoria y se inicializa con un estatus "disponible". 6. Los números y premios resultantes, deben ser almacenados en un archivo o base de datos de premios, registrando básicamente el número participante y el monto del premio cifrado en 3DES para protección de información de los premios.
Algoritmo de Generación Aleatoria de Números Participantes	1. Seleccionar de forma aleatoria números participantes del archivo o base de datos de premios del universo de números disponibles. Más adelante veremos que el concepto también se puede extender a la selección de una terminación (0-9) 2. La cantidad de números seleccionados es determinada por un

[9] **Java Platform 2, Standard Edition** es una colección de APIs del lenguaje de programación Java útiles para muchos programas de la Plataforma Java.

	parámetro de entrada (parametrizable). 3. En caso de que la selección de números sea por terminación, esta es determinada por un parámetro de entrada (parametrizable). 4. Los números participantes en todos los casos son seleccionados al azar, aun cuando la mecánica sea por terminaciones. 5. El algoritmo considera que la generación aleatoria de números participantes es en línea y en paralelo, es decir que diversos procesos pueden estar ejecutando el algoritmo en tiempo real por lo que éste debe considerar la reservación de sus respectivos números participantes (actualiza los números seleccionados a estatus "reservado") 6. El algoritmo es capaz de seleccionar los números participantes, sólo entre aquellos que no hayan sido marcados previamente por el programa de validación de premios como números vendidos o bien no hayan sido reservados por otro proceso en paralelo.
Algoritmo de Validación de Premios.	1. Cuando el usuario selecciona un número de la lista de billetes electrónicos aleatorios mostrados, se realiza un proceso para actualizar el estatus de los números no escogidos a "disponibles", lo que significa que dichos números podrán participar nuevamente en otro proceso de generación aleatoria de números participantes. 2. El número participante seleccionado se registra en la base de datos de premios con estatus "vendido", junto con datos adicionales de la venta (usuario que realizó dicha transacción, fecha, hora, etc.) 3. Se ejecuta un proceso que descifra la información del premio asignado al número participante (recordemos que en el archivo y/o base de datos de premios estos se encuentran cifrados en 3DES). 4. El sistema mediante un algoritmo propio crea un mensaje que contendrá la información del premio relacionado al billete electrónico, tal como premio neto, premio bruto y total de impuestos, y lo cifra con un algoritmo DES (a este proceso se le conoce como "cifrado en el medio")
Generales	A fin de facilitar la generación de evidencias que se solicitan a LOTENAL en procesos de auditorías, las Loterías Electrónicas incluyen: 1. Interfaces Gráficas del Protocolo de Inicio de Sorteos (LOTENAL, Distribuidor) 2. Interfaces Gráficas de Protocolo de Cierre de Sorteo (LOTENAL, Distribuidor). Esta aplicación/sistema permite cargar la base de datos con los billetes devueltos a fin de poder consultar los números participantes vendidos, reservados y disponibles, monto de sus premios, así como datos de seguridad (usuarios que realizaron la transacción, fecha y hora en que se realizaron las transacciones, etc.) una vez que se hayan cerrado los sorteos. 3. Procesos automatizados para el cierre y conciliación final de sorteos (devolución de billetes electrónicos) que permite conciliar el reporte de la venta diaria que efectúa el Distribuidor contra la información de los números vendidos y montos de sus premios de la base de datos de premios una vez que se haya cerrado el sorteo (devolución de billetes electrónicos).

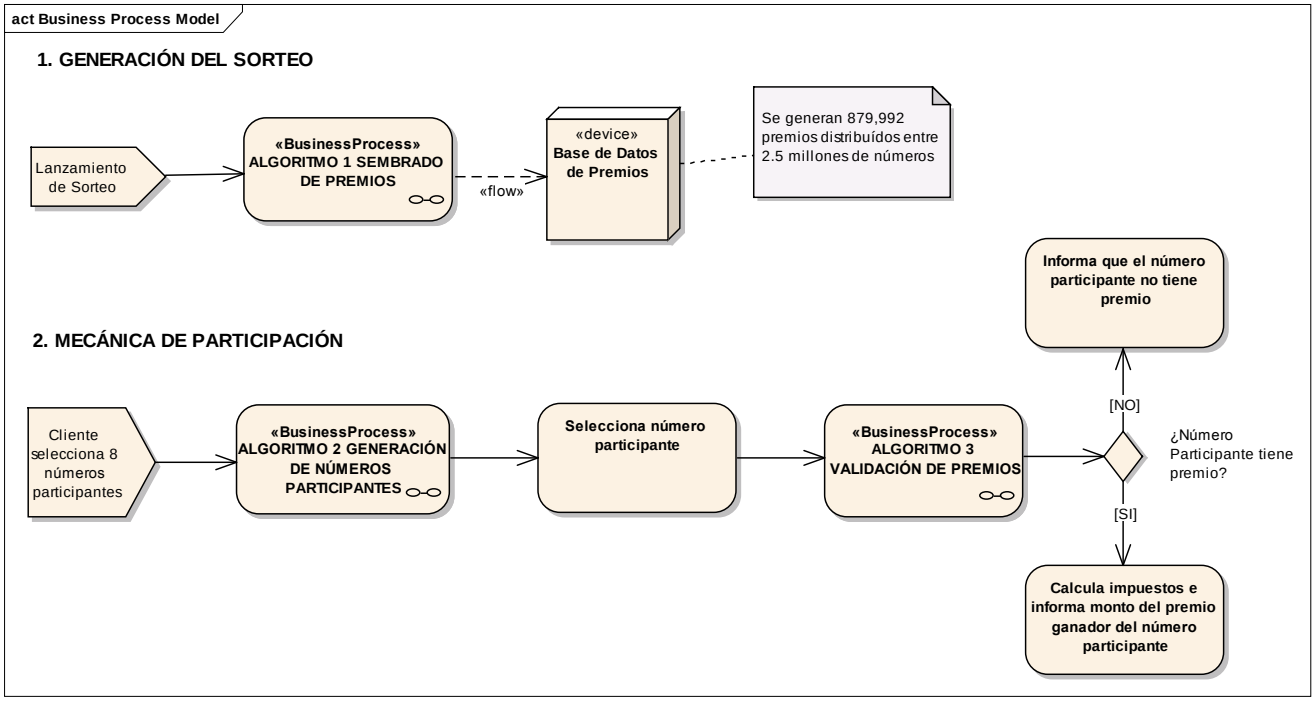


Figura 3.2 Esquema general de Operación de Algoritmos

2.1 Lenguaje Java

Las Loterías Electrónicas se implementaron usando el lenguaje java J2SE 1.3, a continuación revisaremos algo de historia para conocer un poco de este lenguaje y sus características.

2.1.1 Breve historia del Lenguaje Java

Java es un lenguaje de programación orientado a objetos desarrollado por Sun Microsystems a principio de los años 90´s.

El lenguaje Java así como la máquina virtual, comenzaron como un proyecto interno de Sun Microsystems. Los ingenieros de Sun no estaban satisfechos con el rendimiento del lenguaje C++, por lo que James Gosling, Mike Sheridan y Patrick Naughton, junto con otros más, comenzaron a desarrollar un nuevo lenguaje, que en principio pensaron dedicar a la programación de todo tipo de aparatos, tales como microondas, refrigeradores, teléfonos móviles, etc. Ellos pensaban que éstos generarían muchas e importantes aplicaciones para la tecnología del futuro.

El lenguaje tendría que obviar problemas que presenta C++, en campos tales como la programación distribuida, las aplicaciones multi-hilo, el manejo de la memoria y ser más sencillo de manejar que C++. Finalmente se deseaba que los programas fueran portables a todo tipo de aparatos.

Inicialmente el lenguaje se llamó Oak (en español “roble”), en honor de un roble que había frente a la oficina.

En 1992, se presentó como demostración una PDA[10] con interfaz gráfica y un asistente inteligente representado mediante un muñeco llamado Duke.

Oak fue presentado a concurso, como solución tecnológica, en varios proyectos para la industria del cine y la televisión, pero no fue elegido. En 1994 John Gage, James Gosling, Bill Joy, Patrick Naughton, Wayne Rosing, y Eric Schmidt se reunieron para reorientar Oak, y decidieron orientarlo

[10] **Personal Digital Assistant** (asistente digital personal)), es una computadora de mano originalmente diseñada como agenda electrónica (calendario, lista de contactos, bloc de notas y recordatorios) con un sistema de reconocimiento de escritura.

hacia la tecnología de la Web, pues se pensaba que tras la aparición del navegador Mosaic, ésta evolucionaría hacia la misma clase de interactividad, que la televisión por cable, para la cual habían estado preparando Oak.

Fue en 1994 cuando se cambió el nombre de Oak a Java por cuestiones de propiedad intelectual, al existir ya un lenguaje con ese nombre. Se supone que le pusieron así mientras tomaban café (Java es nombre de un tipo de café, originario de Asia), aunque otros afirman que el nombre deriva de las siglas de *James Gosling, Arthur Van Hoff, y Andy Bechtolsheim*.

Poco después, y aún en 1994, la plataforma Java 1.0, estaba disponible para descarga en la Web.

En 1995 Netscape anunció que incluiría soporte para Java en sus navegadores, lo cual fue el factor clave que lanzó a Java a ser conocido y famoso. Como parte de su estrategia de crecimiento mundial y para favorecer la promoción de la nueva tecnología, SUN otorgó permisos a otras compañías para que pudieran tener acceso al código fuente y al mismo tiempo mejorar sus navegadores.
También les permitía crear herramientas de desarrollo para programación Java y los facultaba para acondicionar máquinas virtuales Java (JVM), a varios sistemas operativos.
Muy pronto las licencias o permisos contemplaron prestigiosas firmas como: IBM, Microsoft, Symantec, Silicon Graphics, Oracle, Toshiba y Novell,

Hoy en día, la tecnología Java se puede encontrar en redes y dispositivos que comprenden desde Internet y diversos tipos de máquinas hasta portátiles y teléfonos móviles; desde simuladores de mercado en Wall Street hasta juegos de uso doméstico y tarjetas de crédito, así que podemos decir que “Java está en todas partes”.

2.1.2 Características del Lenguaje Java

Las características del lenguaje Java son las siguientes:

- Orientado a Objetos: Java fue diseñado desde el principio como un lenguaje orientado a objetos. Los objetos agrupan en estructuras encapsuladas tanto sus datos como los métodos (o funciones) que manipulan esos datos.

- Distribuido: Java proporciona una colección de clases para su uso en aplicaciones de red, que permiten abrir sockets y establecer y aceptar conexiones con servidores o clientes remotos, facilitando así la creación de aplicaciones distribuidas.

- Interpretado y compilado a la vez: Java es compilado, en la medida en que su código fuente se transforma en una especie de código máquina (los bytecodes) semejantes a las instrucciones de lenguaje ensamblador. Por otra parte, es interpretado, ya que los bytecodes se pueden ejecutar directamente sobre cualquier máquina en la cual se hayan instalado el intérprete y el sistema de ejecución en tiempo real (run-time).

- Robusto: Java fue diseñado para crear software altamente fiable, para ello proporciona numerosas comprobaciones en compilación y en tiempo de ejecución. Sus características de memoria liberan a los programadores del manejo de aritmética de punteros (los punteros son completamente eliminados del lenguaje) y del manejo de recursos en memoria, ya que el recolector de basura elimina la necesidad de liberación explícita de memoria.

- Portable y Multiplataforma: Java está diseñado para soportar aplicaciones que serán ejecutadas en los más variados entornos de red, desde Unix a Windows Nt, pasando por Mac y estaciones de trabajo, sobre arquitecturas distintas y con sistemas operativos diversos.

- Multi-hilos: Java soporta sincronización de múltiples hilos de ejecución (multithreading) a nivel de lenguaje, especialmente útiles en la creación de aplicaciones de red distribuidas. De esta forma, mientras un hilo se encarga de la comunicación, otro puede interactuar con el usuario mientras otro presenta una animación en pantalla y otro realiza cálculos.

2.1.3 ¿Porqué utilizar Java como lenguaje de implementación en Loterías Electrónicas?

Si bien es cierto que existen muchos lenguajes de programación en el mercado y que cualquiera de ellos podía ser utilizado, las características del lenguaje Java se amoldaban perfectamente a las necesidades y expectativas de Loterías Electrónicas (aplicaciones distribuidas, multiplataforma, multi-hilos) y permitía la implementación del código de una manera sencilla y natural.

Hay que reconocer también que la tendencia de desarrollo en aquella época (2003) era cambiar de la programación estructurada a la programación orientada a objetos, y Java en aquel momento era el lenguaje orientado a objetos de "moda" por ser fácil de aprender, en comparación con el popular C++.

En efecto, la respuesta a la pregunta es que Java encapsulaba en su funcionalidad la solución de las principales dificultades que podría enfrentar el programador, y además era el lenguaje más popular del momento.

2.2 Arquitectura Cliente/Servidor de Loterías Electrónicas

A nivel operación del sorteo (recordemos que el software contiene también procesos de creación, monitoreo y cierre del mismo) las Loterías Electrónicas consisten en servicios expuestos que son instalados en un servidor y que están a la espera de la solicitud de un cliente. Las solicitudes o servicios pueden ser los siguientes:

- Solicitud de Generación de Números Participantes
- Solicitud de Validación de Premios

Cualquiera de estas solicitudes a las Loterías Electrónicas es realizada a través del Distribuidor, el cual recibirá, procesará y enviará la respuesta hacia la Institución Bancaria o Punto de Venta del cual se trate.

Para procesar y dar respuesta a las múltiples solicitudes del Distribuidor hacia las Loterías Electrónicas se desarrolló un servidor de peticiones basado en el protocolo TCP/IP y construido a partir de los APIs[11] java.net del J2SE 1.3

La clase java utilizada en la construcción del servidor fue java.net.Socket. Un Socket es un "canal de comunicación" entre dos programas que corren ya sea en la misma máquina o sobre servidores o máquinas distintas.

Cuando las Loterías Electrónicas son instaladas en una máquina, se ejecuta un proceso para inicializar y levantar el servidor de peticiones en un puerto definido previamente en un archivo de propiedades. El servidor quedará "escuchando" las solicitudes de los clientes (realizadas mediante el Distribuidor) y cuando estas lleguen las asignará a diferentes hilos de ejecución para su procesamiento (Threads[12]).

[11] **Application Programming Interface** es el conjunto de funciones, procedimientos o métodos que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.
[12] Hilo de ejecución o subproceso.

Las solicitudes, como ya lo hemos mencionado, pueden ser de generación de números aleatorios, de terminación, de validación de premios, etc.

El Distribuidor deberá tener un programa cliente que se conecte al servidor de peticiones mediante la dirección IP de la máquina donde éste se encuentre instalado y el puerto donde éste “escucha”.

La comunicación entre cliente y servidor de peticiones está basada en una mensajería con un formato establecido y definido por LOTENAL y el Distribuidor. La información que reciben y envían son cadenas de texto (en java objetos String).

Cuando el servidor de peticiones contesta una solicitud del Distribuidor, le envía una cadena de texto con un formato de posiciones e identificadores que éste sabe interpretar, dependiendo del tipo de solicitud que se hizo, y es el Distribuidor el responsable de procesarla para que sea mostrada adecuadamente al usuario en el punto de venta (cajero automático) recordemos que este proceso es en línea.

Para asegurar la confidencialidad de la información, se utiliza un mecanismo de cifrado DES para la transferencia de datos entre el Distribuidor y LOTENAL a fin de prevenir posibles fraudes (llamado seguridad en el medio).

2.2.1 ¿Por qué utilizar un servidor de peticiones desarrollado en java y no una Aplicación Web?

Los sorteos de Loterías Electrónicas se realizan en tiempo real. Cuando un usuario decide jugar en un cajero automático la generación de números aleatorios y validación de premios debe ejecutarse en segundos, para dar al cliente la imagen de un juego innovador e instantáneo, que le proporcione un sentir de emoción y lo motive a seguir participando.

Recordemos que el ciclo completo de participación involucra 2 acciones:

- El usuario frente al cajero automático decide participar y este le muestra en pantalla 8 números (cada uno correspondiente a un billete electrónico)
- El usuario selecciona el número participante de su agrado y el cajero después de unos segundos muestra los resultados del sorteo. En caso de haber seleccionado un número (billete) ganador, muestra el monto del premio, el cual se abona inmediatamente a la cuenta del usuario.

Pues bien, por cada una de estas solicitudes, la Institución Bancaria envía la petición del servicio al Distribuidor, este la traduce y la envía al servidor de peticiones de Loterías Electrónicas el cual le asigna un hilo de ejecución y realiza el proceso correspondiente (generación o validación de premios). Una vez procesada la solicitud, el servidor de peticiones regresa la respuesta al Distribuidor, en el caso de una validación de premios la respuesta se envía cifrada en DES por cuestiones de seguridad, y el Distribuidor se encarga de procesarla y enviarla a la Institución Bancaria para que se muestre al usuario en el cajero automático.

Debido al dinamismo con el que son desarrolladas las aplicaciones web hoy en día, el tiempo de descarga de las mismas debe ser calculado sobre la marcha. Por lo que la demora de visualización o de obtención de datos no depende solamente del tiempo de descarga sino también del rendimiento del servidor o servidores involucrados.

En la actualidad, es muy común que los sitios Web interactúen con bases de datos, lo que hace que el proceso de descarga o de obtención de datos sea aún más lento, pero todas estas cuestiones técnicas no le interesan al usuario, lo único que ven y perciben es que el sitio que están visitando no les está dando un buen servicio.

Los tiempos de respuesta lentos se traducen directamente en un nivel de confianza menor.

En general los factores que influyen en la velocidad de carga de una página son:

- Rendimiento del Servidor
- Conexión del Servidor con Internet
- Internet
- Conexión del Usuario con Internet
- Velocidad del Navegador y de la Computadora del Usuario

Esto significa que cada uno de estos eslabones aporta su propia cuota de demora, y como las demoras son acumulativas, no se podrán conseguir buenos tiempos de respuesta mejorando solamente alguna de las partes.

Dentro de los requerimientos del sorteo que fueron resultado del estudio de mercado y encuestas realizadas a los usuarios se llegó a la conclusión de que más de 6 segundos por juego en un cajero automático generaría descontento entre aquellos que están esperando su turno en la fila para realizar alguna operación, lo que dañaría la imagen del producto.

Dado lo anterior, los algoritmos de Lotería Electrónica deberían ser capaces de dar respuesta a múltiples transacciones en un tiempo no mayor a 3 segundos, para que el Distribuidor tuviera otros 3 segundos en procesarla y enviarla a la Institución Bancaria.

Por este motivo se consideró mejor solución el desarrollo de un software diseñado como una aplicación autónoma, con tecnología java y basado en una arquitectura Cliente/Servidor, el cual sería responsable de atender las múltiples solicitudes de los clientes.

La infraestructura de LOTENAL, así como los acuerdos pactados con el Distribuidor permitieron establecer un canal de comunicación directo entre ellos mediante una VPN[13] segura y dedicada exclusivamente a responder solicitudes de sorteos electrónicos, lo cual agilizó mucho el tiempo de respuesta del servidor de peticiones hacia el Distribuidor. Además, como canal de comunicación seguro, proporcionaba la certeza de que la información de los premios viajaría íntegra minimizando las posibilidades de amenazas “hackers”.

Véase el siguiente diagrama:

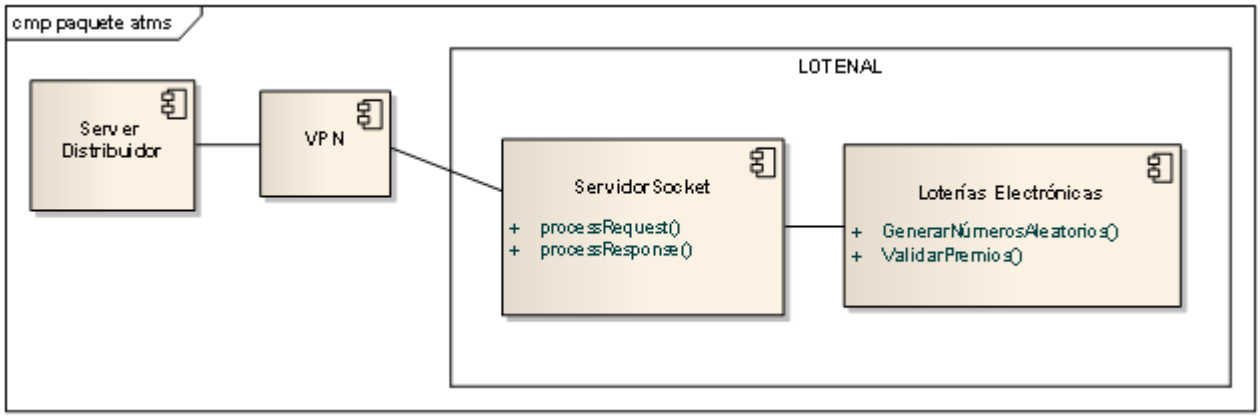


Figura 3.3 Diagrama de Componentes Loterías Electrónicas

Para concluir este capítulo, hablaremos un poco de los procedimientos institucionales de apertura y cierre de sorteo, conocidos como “Protocolos” (recordemos que el software también proporciona interfaces desarrolladas con el API javax.swing, java 1.3.1 para facilitar estos Procedimientos)

[13] Red privada virtual (**virtual private network**), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet. Para que ésta sea segura es necesario proporcionar medios que garanticen la autentificación, integridad y confidencialidad de toda la comunicación:

2.3 Protocolos Normativos de Celebración de Sorteos

Consisten en los procedimientos institucionales con los cuales se da inicio y cierre a los sorteos electrónicos. Estos procedimientos fueron definidos por LOTENAL, en base a la normatividad y regulación de sorteos. Se incluyen en este trabajo debido a que el software de Loterías Electrónicas contiene también los módulos del sistema que operan los usuarios para realizar estas actividades.

2.3.1 Protocolo de Celebración de Sorteos (Sembrado de Premios)

Es la ceremonia que realiza LOTENAL ante las autoridades de Gobernación con la cual dan inicio a un sorteo electrónico. Consiste en los siguientes pasos:

1. Se reúnen los representantes de las diversas áreas de LOTENAL junto con un interventor de la Secretaría de Gobernación para arrancar oficialmente el sorteo. Las áreas son:

    - Dirección General
    - Subdirección General de Finanzas y Sistemas
    - Subdirección General Jurídica
    - Subdirección General de Comercialización y Servicios
    - SEGOB

2. El área de Seguridad Informática a través de la Unidad Certificadora ENTRUST genera certificados digitales para cada uno de los representantes de área que les servirán para acceder al sistema de generación de sorteos. Los certificados son entregados en sobres cerrados.

3. Al acceder al sistema de generación de sorteos, este solicita los datos del certificado digital de cada uno de los representantes de área, junto con un password secreto que reforzará la seguridad.

4. Al ser autenticados por el sistema, cada uno de los representantes de área deberán guardar el certificado digital y el password en el mismo sobre que les fue proporcionado.

5. El sistema genera las siguientes llaves de cifrado:

    - Llave DES (cifrado en el medio)
    - Llave 3DES (cifrado de premios)

6. El sistema realiza el Algoritmo de Sembrado de Premios, el cual genera la base de datos de premios cifrada con la llave 3DES.

7. El sistema imprime un reporte de cifras de control en el cual registra el total de billetes electrónicos generados y el total de premios asignados, el cual debe coincidir con la estructura de premios utilizada en la generación del sorteo.

8. El sistema realiza 2 copias de la base de datos de premios generada por el Sembrado y las almacena en una cinta, a las que llamaremos “cinta origen” y “cinta testigo”.

9. Las evidencias de la generación del sorteo, tales como certificados digitales, reporte de cifras de control, cinta de premios origen y cinta de premios testigo, se resguardan en la Bóveda de Seguridad de la LOTENAL.

Figura 3.4 Protocolo Sembrado de Premios

2.3.2 Protocolo de Carga de Base de Datos

Es la ceremonia que se realiza en las instalaciones del Distribuidor, para instalar en sus sistemas el sorteo electrónico. Recordemos que el Distribuidor es la entidad que proporciona la infraestructura de comunicación entre el sorteo y los puntos de venta (cajeros automáticos).

Los pasos del Protocolo son los siguientes:

1. Se reúnen en LOTENAL los representantes de las diversas áreas involucradas junto con un interventor de la Secretaría de Gobernación y extraen de la Bóveda de Seguridad los sobres que contienen los certificados digitales y la cinta origen con la información de la base de datos de premios cifrados.

2. Se trasladan a las Instalaciones del Distribuidor.

3. En el Distribuidor, cada uno de los representantes de las áreas accede al sistema de Carga de Base de Datos del Sorteo mediante los certificados digitales y los passwords asignados.

4. Se introduce la cinta testigo del sorteo y el sistema realiza el proceso de la Carga de Base de Datos en el servidor del Distribuidor.

5. Una vez cargada la Base de Datos, el sistema genera un reporte de cifras de control en el cual se registra el total de billetes electrónicos cargados y el total de premios asignados, el cual corresponde a la Estructura de Premios Autorizada por LOTENAL.

6. Se ejecutan los procesos necesarios que habilitan el servidor de peticiones, el cual queda activo esperando las solicitudes de venta de los usuarios. En este punto es cuando oficialmente el sorteo ha comenzado su ciclo de vida.

7. Los representantes de las áreas regresan a LOTENAL y vuelven a guardar en la Bóveda de Seguridad los sobres con los certificados digitales, la cinta testigo de los premios del sorteo y el reporte de cifras de control generado por el sistema.

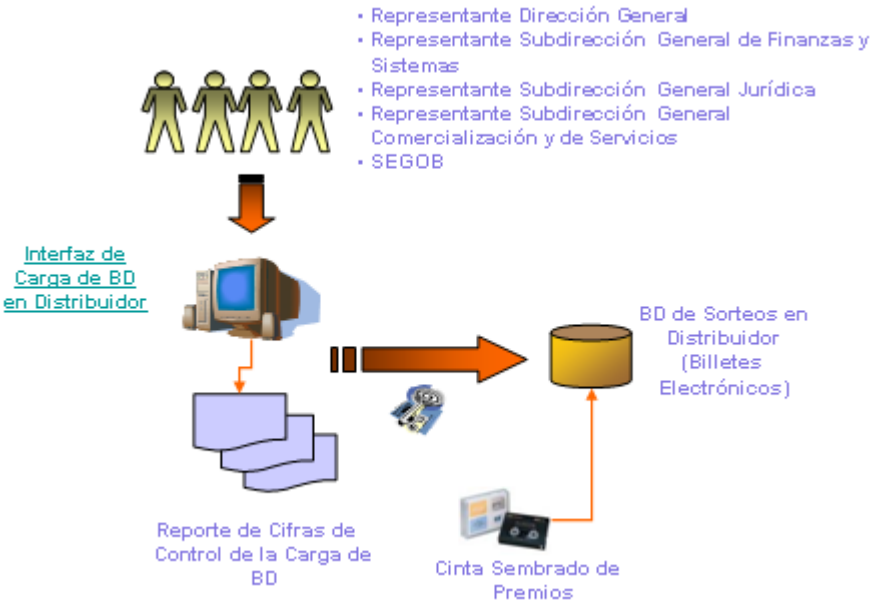


Figura 3.5 Protocolo de Carga de Base de Datos

2.3.3 Protocolo de Cierre de Sorteos (Distribuidor)

Es la ceremonia que se realiza en las instalaciones del Distribuidor cuando el sorteo ha cerrado sus ventas a los usuarios. La finalidad de este proceso es generar una cinta magnética que contenga la información de las transacciones realizadas durante el sorteo (ventas, cancelaciones, etc.), y también generar un reporte de cifras de control que garanticen el funcionamiento correcto del aplicativo.

La información contenida en la cinta será muy importante porque representa el comportamiento del sorteo mientras estuvo vigente, por lo que su generación debe llevarse a cabo en base a ciertos protocolos y políticas de Seguridad definidas previamente por LOTENAL y por el Distribuidor.

Los pasos del Protocolo son los siguientes:

1. Se reúnen en LOTENAL los representantes de las diversas áreas involucradas junto con un interventor de la Secretaría de Gobernación y extraen de la Bóveda de Seguridad los sobres que contienen los certificados digitales y la cinta testigo con la información de la base de datos de premios cifrados.

2. Se trasladan a las Instalaciones del Distribuidor.

3. En el Distribuidor, cada uno de los representantes de las áreas accede al sistema de Cierre de Sorteos mediante los certificados digitales y los passwords asignados.

4. El sistema de Cierre de Sorteos genera una nueva cinta llamada “cinta de Base de Datos devuelta”. Esta cinta contiene la información de las transacciones realizadas por los usuarios en todo el ciclo de vida del sorteo.

5. El sistema genera un reporte de cifras de control que indica los siguientes totales:
   - Billetes electrónicos vendidos
   - Billetes electrónicos reservados
   - Billetes electrónicos disponibles

6. Total de premios otorgados clasificados por monto de premios. Estos premios deben corresponder a la Estructura de Premios autorizada por LOTENAL.

7. Los representantes de las áreas y el interventor de la Secretaría de Gobernación se trasladan a las instalaciones de LOTENAL con los certificados digitales, la cinta Testigo del Sembrado de Premios y la cinta de Base de Datos Devuelta del sorteo.

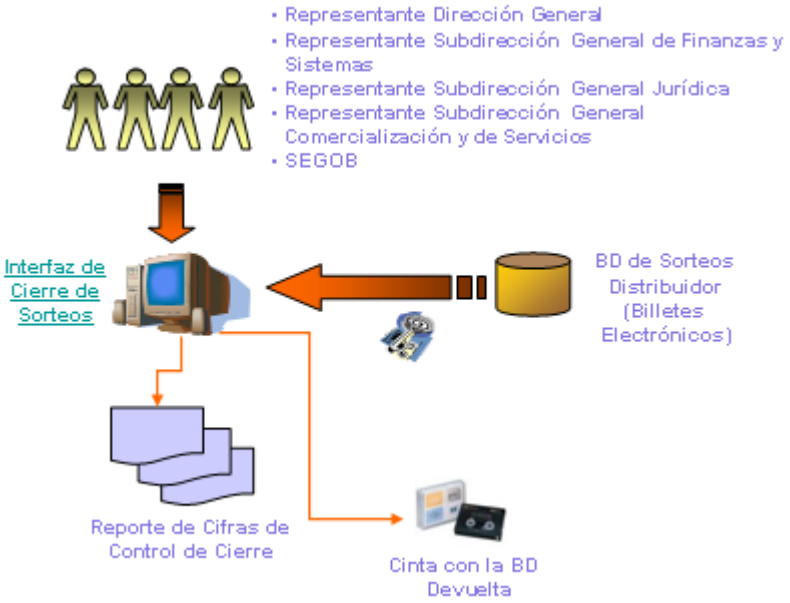


Figura 3.6 Protocolo de Cierre de Sorteos (Distribuidor)

2.3.4 Protocolo de Cierre de Sorteos LOTENAL (Carga de Base de Datos Devuelta)

Esta ceremonia se realiza después del Protocolo de Cierre de Sorteos en el Distribuidor, generalmente el mismo día, en las instalaciones de LOTENAL y su objetivo es validar que la Base de Datos final de transacciones del sorteo reportada por el Distribuidor corresponda en información a la Base de Datos original, sembrada en LOTENAL, es decir, verificar que no haya sido alterada en algún momento durante la vigencia del sorteo.

Los pasos del Protocolo son los siguientes:

1. Los representantes de las diversas áreas de LOTENAL junto con el interventor de la Secretaría de Gobernación arriban a las instalaciones de LOTENAL, con los certificados digitales, la cinta Testigo y la cinta de Base de Datos Devuelta generada en el Distribuidor.

2. Cada uno de los representantes de las áreas accede al sistema de Cierre de Sorteos en LOTENAL mediante los certificados digitales y los passwords asignados.

3. El sistema realiza un proceso con la cinta Testigo generada en el Sembrado de Premios y la cinta de Base de Datos Devuelta entregado por el Distribuidor, para validar lo siguiente:

   - Ambas cintas deben contener la misma información de los billetes electrónicos (misma emisión)
   - En ambas cintas debe coincidir el premio asignado por cada número participante

   Este proceso registra la información de las ventas en la Base de Datos de Sorteos de LOTENAL, y permite garantizar la integridad de la información de ventas, es decir, que los billetes y premios emitidos de inicio correspondan a los billetes y premios entregados por el Distribuidor en las transacciones de venta.

8. El sistema genera un reporte de cifras de control que con las estadísticas de la información contenida en la Base de Datos de sorteos de LOTENAL al final del proceso.

9. Los involucrados firman el Acta Oficial del Cierre del Sorteo y los certificados digitales, las cintas magnéticas generadas, así como los reportes de cifras de Control se guardan nuevamente en la Bóveda de Seguridad de LOTENAL, la cual los conserva como evidencia para futuras aclaraciones o auditorías.

Figura 3.7 Protocolo de Cierre de Sorteos LOTENAL

Capítulo 4. Estudios estadísticos de Pseudo Aleatoriedad

1 Introducción

En la implementación de los algoritmos de Sembrado de Premios y Generación de Números Participantes se utilizó la función “Random” del lenguaje java, por su rapidez y sencillez, sin embargo, cualquier función o programa elaborado en lenguajes de programación, por las misma características de la tecnología informática, no simula completamente la aleatoriedad; pues recordemos que un evento aleatorio, no depende de ninguna condición que sea modelable.

En este capítulo se pretende demostrar que el uso de esta función proporciona un número arbitrario, y que no está sesgada, es decir, que no tiene tendencia hacia ningún número y que los números se repiten con la misma frecuencia. Para demostrar este tipo de situaciones, se requirió elaborar un análisis estadístico basado en Pruebas de Bondad de Ajuste.

A continuación se detalla el análisis de confiabilidad realizado:

2 Análisis de Confiabilidad de la clase Random del paquete java.util del JDK 1.3.1

2.1 Pruebas de Bondad de Ajuste.

En este tipo de pruebas se busca establecer si las diferencias observadas entre los datos reales y los teóricos se deben al azar, o si por el contrario la teoría no es buena para explicar la realidad. A eso se le llama Pruebas de Bondad de Ajuste.

Cuando los supuestos no se cumplen, o sencillamente por su facilidad de ejecución, la prueba más recomendable en el campo de la estadística no paramétrica es la de Kolmogorov-Smirnov, para una y para comparar dos muestras entre sí. Este modelo es el que será aplicado para nuestro problema en particular y a continuación se describe. En esencia se utilizará la prueba de Kolmogorov-Smirnov para dos muestras.

2.2 Estadística de Kolmogorov-Smirnov.

Si se desea comparar si dos o más muestras son gobernadas por la misma distribución desconocida, suena natural comparar la distribución empírica de las funciones de distribución de esas muestras para determinar si guardan alguna similitud.

La prueba de Kolmogorov-Smirnov para dos muestras, es un modelo estadístico para verificar si dos muestras independientes han sido extraídas de la misma población o de poblaciones con igual función de distribución, nosotros deseamos verificar que cada uno de los números aparece con la misma frecuencia, es decir, los números tienen la misma función de distribución y por lo tanto no son tendenciosos, es decir, no existen números que aparezcan una mayor cantidad de veces que los demás.

Es decir, si logramos probar que las muestras provienen de la misma población, entonces son aleatorias e independientes, por lo tanto, los números son arbitrarios.

La prueba de dos colas es sensible a cualquier clase de diferencia entre las distribuciones de donde fueron extraídas ambas muestras, La prueba de una cola se usa para decidir si los valores de la población de donde se extrajo a una de las muestras, son estocásticamente mayores (o menores) que las de la otra población.

2.2.1 Datos

Los datos consisten en dos muestras aleatorias independientes, una de tamaño n, X1, X2,…, Xn, y otra de tamaño m, Y1, Y2,…, Ym. Sean F(x) y G(x) sus respectivas funciones de distribución desconocidas.

2.2.2 Suposiciones

1. Las muestras son muestras aleatorias.
2. Las dos muestras son mutuamente independientes.
3. La escala de medida es al menos ordinal.
4. Para ser exactos en esta prueba se asume que las variables aleatorias son continuas. Si las variables aleatorias son discretas, la prueba es válida pero se vuelve conservadora.

2.2.3 Estadístico de Prueba.

Sea S1(x) la función de distribución empírica basada en la muestra aleatoria X1, X2,…, Xn y sea S2(x) la función de distribución empírica de la muestra aleatoria Y1, Y2,…, Ym. El estadístico de prueba es definido como sigue:

A. (Prueba de dos colas). Se define el estadístico de prueba T1 como la distancia vertical más grande entre las dos funciones de distribución empíricas.

$$T_1 = \sup| S_1(x) - S_2(x)|$$

2.2.4 Hipótesis.

A. (Prueba de dos colas).

H_0: $F(x) = G(x)$ para todo x desde $-\infty$ a ∞

H_1: $F(x) \neq G(x)$ para al menos un valor de x

Se rechaza H_0 al nivel de significancia α si T_1 es mayor que el cuantil $1 - \alpha$ para una prueba de dos colas, dada la tabla I para m = n, ó por la tabla II, para m ≠ n. Use la aproximación al final de las tablas para una muestra de tamaño más grande no cubierta por las tablas. Ver tablas de valores críticos al final del capítulo.

Es decir, dadas dos muestras aleatorias, mutuamente independientes, la hipótesis nula es que si la muestra A tiene una función de distribución F(x) y la muestra B tiene una función de distribución G(x), entonces la función de distribución es la misma para cualquier valor de las variables o provienen de la misma población, versus la hipótesis alterna de que al menos para un valor de las variables las funciones de distribución son distintas.

Para desarrollar este modelo se deben seguir los siguientes pasos:

- Se ordena cada grupo en orden ascendente. Con el rango se obtiene el número de clases, como en los histogramas, pero tratando de tener el mayor número de clases posible, para ambas muestras.

- Se calculan las frecuencias de cada grupo de las mismas clases, luego sus frecuencias acumuladas y finalmente, dividiendo por el respectivo tamaño muestral, se calculan las frecuencias acumuladas relativas.

- Para cada clase, se calculan las diferencias en valor absoluto de las frecuencias acumuladas relativas de cada grupo. Y se busca el valor máximo, dado que las funciones son discretas, el supremo coincide con el máximo, de esas diferencias T_1.

- Se determina el valor correspondiente en la tabla de valores críticos. Ver tablas de valores críticos al final del capítulo.

- Se comparan estos valores críticos con el estadístico T_1 de Kolmogorov-Smirnov para dos muestras. Ver tablas de valores críticos al final del capítulo.

Dado que la función de distribución que requerimos es de tipo discreta, se aplica una corrección por no continuidad, la cual está dada por:

$T_1 = \lambda [(m+n)/mn]^{1/2}$ si $m \neq n$, y como

$T_1 = \lambda / n^{1/2}$ si $m = n$

Donde λ es el valor en tablas para el quantil α y m,n son los tamaños de las muestras respectivas.

2.2.5 Tamaño de la muestra.

El propósito de la teoría del muestreo es que éste sea más eficiente. Su objetivo es desarrollar métodos de selección de muestras y de estimación, que proporcionen, al menor costo posible, estimaciones con la suficiente exactitud para nuestros propósitos.

La fórmula para calcular el tamaño de la muestra preliminar es la siguiente:

$No = (Z^2 * p * q) / d^2$

Donde:

Z es el nivel de confianza deseado (en este caso Z=1.96, ya que queremos un 95% de confianza).

p es la probabilidad del evento, en este caso, el evento es que el número sea aleatorio o que no lo sea, por lo que el valor de p = 0.5

q es la probabilidad del complemento (es decir, que no salga el número aleatorio), por lo que q = (1–p) = (1–0.5) = 0.5

d es la precisión deseada, es decir al elegir 5% significa que la probabilidad no contiene un error mayor del $\pm$ 5%, es decir nuestra probabilidad se encontrará con certeza en el intervalo [p-5%, p+5%].

Por lo tanto, el tamaño de la muestra preliminar con d=5% es de: **384.16**

2.2.6 Tamaño de la muestra real.

Cuando la población es pequeña, la muestra obtenida mediante la fórmula anterior, es demasiado grande, en estos casos se debe aplicar la siguiente formula correctora:

1/N = 1/No + 1/Tamaño de la Población

Haciendo el ajuste correspondiente el tamaño de la muestra real se calcula mediante la siguiente fórmula:

N = No / (1+ ((No-1)/Tamaño de la Población))

Donde No = 384.16 y Tamaño de la Población = 2,500,000

Por lo que la muestra real es de: **384.10** ~ **384**

Una vez obtenido el tamaño de la muestra, lo que sigue es obtener las muestras con un programa que tome como función aleatoria la clase java.util.Random().

Después de ejecutar el programa mencionado, llegamos a las dos muestras que se presentan en la siguiente tabla.

2.2.7 Tabla con las muestras obtenidas al aplicar la función Random()

#	Muestra 1	Muestra 2	#	Muestra 1	Muestra 2	#	Muestra 1	Muestra 2
1	1625443	1826018	41	186570	1629873	81	260760	944092
2	268157	1697515	42	87789	1784221	82	63888	425613
3	806243	432375	43	1998809	540774	83	728115	2480133
4	1633570	1212749	44	1668467	2428897	84	1815942	937952
5	1552173	386949	45	461295	1139920	85	491071	2205441
6	1447972	1289380	46	2191173	1654742	86	1613107	783295
7	85662	1794869	47	973841	1154922	87	2118596	322120
8	850376	1431723	48	997923	932656	88	134541	244335
9	1252750	1216525	49	399905	849407	89	1848177	1381993
10	2362725	1734206	50	333634	1150742	90	669484	2074128
11	1839910	1221258	51	319229	1090561	91	1866487	2124194
12	2081132	225941	52	1281661	2393971	92	155026	978253
13	1033432	621606	53	882612	792578	93	16549	378491
14	2031986	1675141	54	211992	1032025	94	1228437	2099744
15	2158719	1619306	55	2049606	933298	95	902683	68128
16	1608636	2445196	56	871986	1758418	96	564811	769125
17	293492	2356858	57	2455159	592821	97	482317	2491962
18	1941734	2009680	58	404456	2028036	98	2134001	486713
19	582026	2277197	59	2041807	2153280	99	987606	1230633
20	2292400	2087968	60	2461536	375680	100	183352	309710
21	980903	289294	61	860625	2286640	101	42390	61247
22	741029	1226455	62	874808	1342312	102	1766124	2407374
23	2413631	2229185	63	2129142	1108743	103	1289450	1558203
24	2137097	1260387	64	1300235	1728922	104	1387714	1846762
25	2294382	1087073	65	2049541	1671653	105	1841191	2266113
26	406526	538865	66	143325	2324638	106	670430	1670494
27	1154034	2107895	67	1278898	907999	107	766034	605203
28	1221875	559894	68	2307972	502568	108	23198	812994
29	2088675	2436505	69	56976	616542	109	586846	1851406
30	229354	323164	70	2027155	1456266	110	2258695	468655
31	1157584	1515676	71	754548	696598	111	2440451	408100
32	2471524	1463879	72	1170275	1195129	112	940970	1869868
33	927287	1243991	73	203560	2430113	113	1250424	439089
34	1743500	846691	74	1269856	1500217	114	1581330	278613
35	92993	2131959	75	1920232	459096	115	2376334	1063580
36	657244	2410956	76	537582	2447176	116	1562572	2082919
37	301656	821016	77	735612	1283853	117	506024	1169772
38	2433360	1882905	78	1201559	91877	118	637811	44810
39	720837	898727	79	1687634	2102792	119	934874	970500
40	2086405	2143686	80	1420434	697659	120	1446232	1266299

#	Muestra 1	Muestra 2	#	Muestra 1	Muestra 2	#	Muestra 1	Muestra 2
121	540765	1809597	165	682027	1944443	209	1968466	1968466
122	1139787	2119829	166	141699	1031394	210	783541	783541
123	1193132	207998	167	2091693	2085991	211	1606499	1606499
124	1663528	2138556	168	526881	1479337	212	605207	605207
125	1628574	1543994	169	2498345	1535594	213	1004617	1004617
126	1093312	808774	170	33785	1300209	214	2217256	2217256
127	807712	2346375	171	64634	579302	215	262506	262506
128	700515	747493	172	502524	1132781	216	1429185	1429185
129	1795758	522454	173	2484868	556898	217	606019	606019
130	1476743	2097109	174	844643	870064	218	18982	18982
131	2092046	934260	175	2059189	1014306	219	2432310	2432310
132	1352696	41439	176	312755	1850188	220	819845	819845
133	1752938	2147484	177	959894	1552856	221	1763519	1763519
134	2416380	123176	178	1827596	579510	222	1708412	1708412
135	1685704	276374	179	1297357	145044	223	1644004	1644004
136	1358849	1652665	180	1062958	2315845	224	1269239	1269239
137	1650375	2221488	181	2162259	1282167	225	885738	885738
138	93702	1986859	182	2454409	75322	226	1109014	1109014
139	1829816	2298904	183	820717	1804965	227	674820	674820
140	375555	1624367	184	112959	1206361	228	1998765	1998765
141	2165335	1818835	185	761673	2472569	229	1444615	1444615
142	1155829	1847127	186	187128	466357	230	1130502	1130502
143	2438276	72157	187	129431	1474546	231	1891641	1891641
144	1516682	1719556	188	1045634	240585	232	227585	227585
145	1459682	452637	189	442337	1877675	233	2402663	2402663
146	808325	1056461	190	840291	155235	234	139707	139707
147	2313260	149124	191	444105	1811497	235	1070966	1070966
148	385775	1780297	192	98685	2293115	236	369260	369260
149	2387439	2415267	193	1333789	214253	237	2342673	2342673
150	957851	271898	194	2240508	1831809	238	1446506	1446506
151	1395816	314694	195	1486297	2289097	239	1858049	1858049
152	63891	1859478	196	2412159	122741	240	1924236	1924236
153	985434	387664	197	2370874	2397519	241	1593627	1593627
154	1559172	189939	198	1715712	2392688	242	145833	145833
155	1026283	1838004	199	574586	1971429	243	1630514	1630514
156	65955	722958	200	1256034	561376	244	1443646	1443646
157	2011613	2320077	201	998485	998485	245	2154382	2154382
158	872602	1672855	202	1208624	1208624	246	1655470	1655470
159	1369188	1401147	203	2085697	2085697	247	868533	868533
160	2349428	1368925	204	585126	585126	248	437315	437315
161	2292329	202234	205	2479060	2479060	249	470981	470981
162	1971744	1375698	206	1074405	1074405	250	1414227	1414227
163	1329914	1055009	207	103731	103731	251	1435185	1300355
164	2412389	1237155	208	1377491	1377491	252	287279	839199

#	Muestra 1	Muestra 2	#	Muestra 1	Muestra 2	#	Muestra 1	Muestra 2
253	1926651	2250830	297	794115	746177	341	11460	1193199
254	609696	1384661	298	969454	1936982	342	371090	2156337
255	1079728	312557	299	1138997	1863402	343	1023754	2338706
256	1369594	1453269	300	2215247	1382788	344	318454	306951
257	997779	370919	301	1604531	38476	345	1800381	2478644
258	620027	1434896	302	979594	2339013	346	1689452	1434405
259	1241043	2283665	303	626450	2066516	347	1246751	1170785
260	884280	2254988	304	2101774	1626516	348	1745893	1862625
261	1593313	494945	305	1282309	733178	349	158188	2247164
262	140127	623908	306	1619392	1621452	350	1216362	164673
263	868779	1127458	307	653752	1337909	351	757880	98357
264	821157	2097228	308	785386	966191	352	2371357	712571
265	1038074	2475040	309	5068	1235121	353	311972	589303
266	2180753	1369971	310	2099139	799683	354	1511022	572533
267	1395236	555747	311	221326	1476440	355	2134365	590333
268	2206499	147841	312	1917399	734070	356	298557	1930892
269	1455087	987321	313	1849814	951981	357	252209	297028
270	1187107	1793216	314	2102835	1132547	358	2240134	326960
271	457859	1840940	315	600857	1254137	359	2495342	68795
272	2463682	372183	316	1208815	1564589	360	1627310	910859
273	685291	1300146	317	1858220	967452	361	503033	494103
274	1862607	2454512	318	1374584	113768	362	477832	2123362
275	260840	2407491	319	698038	2243589	363	774376	2082563
276	2203960	784763	320	2152217	360343	364	1253541	1886004
277	980593	910470	321	1546992	713117	365	1222909	2426613
278	819930	1401900	322	43717	381647	366	705142	1024768
279	1597834	1167684	323	976955	993277	367	2277247	391996
280	176296	1434176	324	192004	1823323	368	578687	807748
281	2056384	1918366	325	1278686	1729120	369	47734	174325
282	394932	637309	326	1434744	2429593	370	206425	960320
283	1226111	2012633	327	1070491	36114	371	595907	1857277
284	424157	504919	328	1240938	574657	372	747844	2221464
285	1258129	498647	329	1616877	1593864	373	2150202	1322369
286	237045	2437838	330	401270	1736838	374	2457032	1960440
287	878035	830082	331	1345280	1459850	375	1709437	1450417
288	2335917	324949	332	1703152	1004405	376	627366	2063282
289	1682133	582786	333	1562253	365451	377	1893142	239891
290	131743	1388558	334	1544817	1125115	378	2465888	2038627
291	1420045	1428078	335	1569425	593465	379	374448	1499283
292	2350136	1371952	336	1756930	1779363	380	1575745	1815763
293	2018169	2332543	337	1167177	732592	381	111922	952280
294	1315328	986890	338	2345091	2448412	382	1953290	1603707
295	2402575	1242143	339	1129355	700905	383	2043386	1240338
296	553063	2343650	340	1638233	1210904	384	2088474	812513

2.2.8 Resultados

Con este par de muestras que se obtuvieron con la función Random de java, se siguieron los pasos anteriormente mencionados, para encontrar el estadístico de prueba T_1, obteniéndose la siguiente tabla de resultados:

Clase	Frecuencia Muestra 1	Frecuencia Muestra 2	Frecuencia Relativa Muestra 1	Frecuencia Relativa Muestra 2	Frecuencia Acumulada Muestra 1	Frecuencia Acumulada Muestra 2	ABS(DIF)
11460	2	0	0.005208333	0	0.005208333	0	0.005208333
142348.6842	26	17	0.067708333	0.044270833	0.072916667	0.044270833	0.028645833
273237.3684	21	18	0.0546875	0.046875	0.127604167	0.091145833	0.036458333
404126.0526	17	23	0.044270833	0.059895833	0.171875	0.151041667	0.020833333
535014.7368	16	17	0.041666667	0.044270833	0.213541667	0.1953125	0.018229167
665903.4211	20	23	0.052083333	0.059895833	0.265625	0.255208333	0.010416667
796792.1053	21	17	0.0546875	0.044270833	0.3203125	0.299479167	0.020833333
927680.7895	22	18	0.057291667	0.046875	0.377604167	0.346354167	0.03125
1058569.474	21	24	0.0546875	0.0625	0.432291667	0.408854167	0.0234375
1189458.158	17	18	0.044270833	0.046875	0.4765625	0.455729167	0.020833333
1320346.842	27	25	0.0703125	0.065104167	0.546875	0.520833333	0.026041667
1451235.526	23	25	0.059895833	0.065104167	0.606770833	0.5859375	0.020833333
1582124.211	15	15	0.0390625	0.0390625	0.645833333	0.625	0.020833333
1713012.895	27	20	0.0703125	0.052083333	0.716145833	0.677083333	0.0390625
1843901.579	14	22	0.036458333	0.057291667	0.752604167	0.734375	0.018229167
1974790.263	16	22	0.041666667	0.057291667	0.794270833	0.791666667	0.002604167
2105678.947	22	18	0.057291667	0.046875	0.8515625	0.838541667	0.013020833
2236567.632	17	16	0.044270833	0.041666667	0.895833333	0.880208333	0.015625
2367456.316	15	21	0.0390625	0.0546875	0.934895833	0.934895833	0
y mayor...	25	25	0.065104167	0.065104167	1	1	0

Se tiene que T1 = **0.0390625**, comparando con el valor crítico en tablas (ver Anexo de Tablas de inferencia para 2 muestras del mismo tamaño) se tiene que el valor del estadístico es:

$1.92 / 384^{1/2}$ = **0.09797959**, entonces para un precisión del 5% y un nivel de confianza del 95%, se tiene que:

T1 < kα, por lo tanto aceptamos la hipótesis nula, es decir, las muestras provienen de la misma población, por lo que las muestras son mutuamente independientes y aleatorias, dentro de la misma población, lo que quiere decir que la función Random de java no tiene sesgos.

Por otro lado, para el sembrado de premios, se utiliza un algoritmo aleatorio en el que también interviene la función Random de java, que se ha probado no tiene sesgos, el algoritmo para el sembrado de premios es el siguiente:

2.3 Descripción del algoritmo para Sembrado de Premios

En un principio, se tiene 2,500,000 de números ordenados del 1 al 2,500,000 en orden ascendente, se elige un número con la función Random de java, se saca del conjunto de números y se ordena en un nuevo conjunto, y así sucesivamente hasta que se terminan los números del primer conjunto. De nuevo se ocupará la prueba de hipótesis de Kolmogorov Smirnov, dado que el segundo conjunto, está “desordenado” con respecto al primero, se toman los primeros 384 números de repetir dos

veces este algoritmo para desordenar la población original. Las muestras quedan como en la siguiente tabla:

2.3.1 Tabla con las muestras obtenidas al aplicar la función Random()

#	Muestra 1	Muestra 2	#	Muestra 1	Muestra 2	#	Muestra 1	Muestra 2
1	4214	4236	41	239607	271902	81	479792	534489
2	24855	9211	42	247361	276505	82	481907	542299
3	27586	10853	43	262286	277192	83	484460	555948
4	32853	14606	44	278565	280185	84	489500	562912
5	37164	14654	45	300519	287688	85	499952	566253
6	37888	21253	46	311762	300436	86	500192	570211
7	54085	21540	47	314395	306560	87	501660	589157
8	73640	25833	48	315235	317523	88	507085	592024
9	73893	33440	49	321810	322458	89	517825	600756
10	79151	38513	50	321980	327828	90	524469	627462
11	85002	59241	51	323696	328027	91	536347	629447
12	86053	90187	52	324060	337783	92	539999	638918
13	96566	91487	53	327086	352954	93	542088	648123
14	97753	95805	54	327305	353517	94	549885	661214
15	107519	101958	55	334572	357870	95	562672	681491
16	110246	117997	56	335475	358637	96	564339	693025
17	117347	125124	57	338328	361671	97	565680	699864
18	118694	131182	58	343045	369797	98	568204	700534
19	119658	143354	59	345142	376544	99	569224	703252
20	140677	144243	60	348826	380122	100	573204	707610
21	152433	155611	61	354166	389596	101	576760	707745
22	162545	161819	62	359847	394967	102	578079	731415
23	167464	163555	63	369577	401379	103	595432	737524
24	172082	163804	64	380238	410334	104	596429	748500
25	173903	169314	65	386085	414366	105	605461	752079
26	176397	169935	66	387557	414964	106	613090	770068
27	177272	178075	67	389403	420189	107	615250	770226
28	179765	182523	68	389578	424567	108	615805	772299
29	184730	188298	69	392664	435686	109	618809	788165
30	185052	195960	70	398937	454507	110	619284	789049
31	185308	211214	71	399477	457578	111	621394	790973
32	189695	215211	72	409382	459451	112	631927	792441
33	198897	234897	73	413318	462359	113	634483	802786
34	202010	250134	74	417303	468533	114	637680	802884
35	204066	252343	75	428309	472480	115	642219	810622
36	221914	255121	76	443136	474661	116	642442	815763
37	230314	262289	77	453566	475407	117	643406	820252
38	231385	262910	78	460839	476816	118	648281	824187
39	236746	264186	79	461442	506481	119	648772	824422
40	238066	264670	80	470438	532746	120	648851	832912

#	Muestra 1	Muestra 2	#	Muestra 1	Muestra 2	#	Muestra 1	Muestra 2
121	649075	837474	165	956071	1130467	209	1214316	1375350
122	649297	849734	166	963021	1136156	210	1218977	1375407
123	663271	854221	167	964793	1138488	211	1220812	1375558
124	669667	863277	168	970179	1143891	212	1222931	1381944
125	676043	868161	169	971008	1155038	213	1223343	1385952
126	676770	871113	170	978531	1158801	214	1230389	1386323
127	677286	871778	171	980564	1168995	215	1230757	1390258
128	682165	880091	172	987006	1177206	216	1259181	1392687
129	689199	890467	173	990323	1184790	217	1265715	1396267
130	697108	900830	174	995302	1187332	218	1268611	1426173
131	705228	903630	175	1014231	1189178	219	1272373	1429623
132	706388	908520	176	1015757	1200166	220	1273489	1430746
133	727246	917865	177	1019748	1202383	221	1274924	1430827
134	730261	921923	178	1024405	1209027	222	1275162	1431206
135	738224	926473	179	1025399	1219982	223	1275749	1435109
136	740196	928978	180	1031083	1244244	224	1276263	1461136
137	757078	934109	181	1044431	1271282	225	1297865	1490223
138	759646	938415	182	1045015	1273950	226	1320353	1495302
139	764763	940841	183	1051662	1277332	227	1321540	1504812
140	764848	941321	184	1062601	1279769	228	1373571	1532708
141	774148	942935	185	1065955	1279842	229	1376411	1535074
142	776744	949954	186	1070026	1285758	230	1399047	1537995
143	778859	959142	187	1071371	1286429	231	1405438	1538240
144	786645	967005	188	1081512	1295019	232	1410862	1541176
145	788115	967184	189	1103099	1299902	233	1412450	1544027
146	788265	974785	190	1105404	1302275	234	1421270	1572927
147	808914	979316	191	1107257	1312079	235	1425980	1588001
148	809553	987792	192	1112263	1316216	236	1441756	1595356
149	811858	988672	193	1117583	1318997	237	1444772	1600221
150	815014	991276	194	1118562	1326412	238	1449188	1603005
151	847249	1003262	195	1129174	1326584	239	1449557	1607774
152	853257	1006287	196	1140481	1327103	240	1466525	1611716
153	867900	1008346	197	1141562	1327336	241	1481838	1623148
154	887832	1010013	198	1156856	1335513	242	1488561	1628748
155	889547	1025335	199	1165839	1345586	243	1493108	1643642
156	900893	1031310	200	1179763	1351136	244	1505218	1645262
157	907984	1033226	201	1181599	1352265	245	1506606	1647148
158	914493	1046215	202	1183097	1358779	246	1511207	1653812
159	918765	1081148	203	1183301	1363564	247	1518907	1653905
160	920907	1081544	204	1183651	1364077	248	1524116	1661091
161	926300	1081620	205	1189500	1364517	249	1543688	1665233
162	928774	1083836	206	1190941	1366804	250	1545045	1665726
163	930235	1116079	207	1200803	1368726	251	1545097	1676095
164	931480	1127045	208	1201304	1368761	252	1545328	1677562

#	Muestra 1	Muestra 2	#	Muestra 1	Muestra 2	#	Muestra 1	Muestra 2
253	1551018	1683755	297	1868714	1971286	341	2204207	2218690
254	1559432	1685316	298	1874134	1977060	342	2227413	2220923
255	1560917	1686530	299	1879737	1986381	343	2228658	2226529
256	1565772	1712995	300	1885450	1986499	344	2229220	2227315
257	1569007	1725037	301	1894711	1999199	345	2249617	2228932
258	1576986	1727121	302	1895716	2001484	346	2252302	2230448
259	1587170	1729330	303	1895741	2015179	347	2254275	2238914
260	1590869	1738374	304	1906442	2017860	348	2259945	2239262
261	1592229	1738396	305	1913647	2021186	349	2262886	2245836
262	1600808	1751499	306	1914090	2021595	350	2263220	2245946
263	1606463	1754785	307	1923374	2029054	351	2263269	2247247
264	1609048	1765831	308	1923871	2034636	352	2264890	2260081
265	1628251	1782842	309	1925404	2041268	353	2290788	2264479
266	1631431	1789016	310	1932779	2046151	354	2310466	2268167
267	1635575	1798205	311	1935987	2054467	355	2312623	2269892
268	1636869	1805620	312	1953467	2071450	356	2315807	2278077
269	1640495	1807736	313	1955609	2079975	357	2324339	2287861
270	1642871	1815962	314	1957062	2082293	358	2325036	2288566
271	1647489	1823218	315	1969597	2088902	359	2325771	2326488
272	1648411	1824118	316	1981796	2089598	360	2330249	2342201
273	1670307	1845154	317	1982589	2116011	361	2343552	2351166
274	1683781	1846506	318	1986952	2119511	362	2348024	2358190
275	1684477	1848883	319	1987175	2120848	363	2355377	2365695
276	1685124	1853265	320	2015207	2121481	364	2362205	2372818
277	1691821	1865534	321	2025003	2127653	365	2378632	2379963
278	1696131	1867709	322	2043589	2128219	366	2380717	2384769
279	1707031	1868427	323	2046236	2131108	367	2382767	2391431
280	1708626	1872410	324	2049974	2136022	368	2384324	2395974
281	1714822	1878619	325	2059031	2138662	369	2386976	2397324
282	1721058	1879304	326	2069335	2142809	370	2388569	2397514
283	1732044	1880184	327	2074646	2144978	371	2389571	2399851
284	1741748	1887506	328	2078737	2147789	372	2391905	2401355
285	1742889	1892699	329	2082044	2149403	373	2415317	2408701
286	1745146	1894411	330	2086375	2157563	374	2420832	2408956
287	1759754	1913603	331	2090278	2165376	375	2435886	2418271
288	1766826	1914380	332	2092988	2168209	376	2450936	2432870
289	1781198	1919999	333	2096718	2175328	377	2456263	2435055
290	1796371	1926955	334	2112532	2186843	378	2471087	2442102
291	1802131	1933536	335	2117495	2194229	379	2478037	2454736
292	1803160	1934482	336	2117848	2200029	380	2481097	2455100
293	1850435	1937595	337	2160639	2202007	381	2484414	2467817
294	1853725	1942530	338	2167643	2206343	382	2493652	2472776
295	1858487	1953795	339	2169079	2210729	383	2494440	2492941
296	1862158	1956591	340	2173754	2210908	384	2498575	2497200

2.3.2 Resultados

Con este par de muestras que se obtuvieron de aplicar dos veces el desordenamiento a la población inicial, se siguieron los pasos anteriormente mencionados, para encontrar el estadístico de prueba T_1, obteniéndose la siguiente tabla de resultados:

Clase	Frecuencia Muestra 1	Frecuencia Muestra 2	Frecuencia Relativa Muestra 1	Frecuencia Relativa Muestra 2	Frecuencia Acumulada Muestra 1	Frecuencia Acumulada Muestra 2	ABS(DIF)
4236	1	1	0.002604167	0.002604167	0.002604167	0.002604167	0
135444.63	18	17	0.046875	0.044270833	0.049479167	0.046875	0.002604167
266653.26	24	22	0.0625	0.057291667	0.111979167	0.104166667	0.0078125
397861.89	26	22	0.067708333	0.057291667	0.1796875	0.161458333	0.018229167
529070.53	21	17	0.0546875	0.044270833	0.234375	0.205729167	0.028645833
660279.16	32	14	0.083333333	0.036458333	0.317708333	0.2421875	0.075520833
791487.79	24	18	0.0625	0.046875	0.380208333	0.2890625	0.091145833
922696.42	14	23	0.036458333	0.059895833	0.416666667	0.348958333	0.067708333
1053905.1	23	24	0.059895833	0.0625	0.4765625	0.411458333	0.065104167
1185113.7	21	15	0.0546875	0.0390625	0.53125	0.450520833	0.080729167
1316322.3	21	19	0.0546875	0.049479167	0.5859375	0.5	0.0859375
1447530.9	12	31	0.03125	0.080729167	0.6171875	0.580729167	0.036458333
1578739.6	21	11	0.0546875	0.028645833	0.671875	0.609375	0.0625
1709948.2	22	21	0.057291667	0.0546875	0.729166667	0.6640625	0.065104167
1841156.8	12	17	0.03125	0.044270833	0.760416667	0.708333333	0.052083333
1972365.5	23	25	0.059895833	0.065104167	0.8203125	0.7734375	0.046875
2103574.1	18	19	0.046875	0.049479167	0.8671875	0.822916667	0.044270833
2234782.7	11	30	0.028645833	0.078125	0.895833333	0.901041667	-0.005208333
2365991.4	20	17	0.052083333	0.044270833	0.947916667	0.9453125	0.002604167
y mayor...	20	21	0.052083333	0.0546875	1	1	0

Se tiene que T1 = **0.09114583**, comparando con el valor crítico en tablas (ver Anexo de Tablas de inferencia para 2 muestras del mismo tamaño) se tiene que el valor del estadístico es:

$1.92 / 384^{1/2}$ = **0.09797959**, entonces para un precisión del 5% y un nivel de confianza del 95%, se tiene que:

$T1 < k\alpha$, por lo tanto aceptamos la hipótesis nula, es decir, las muestras provienen de la misma población, por lo que las muestras son mutuamente independientes y aleatorias, dentro de la misma población, lo que quiere decir que el algoritmo no tiene sesgos.

2.4 Conclusiones.

Dados los anteriores resultados se concluye que los algoritmos y funciones utilizadas, para la Generación de Números Aleatorios y Sembrado de Premios son arbitrarios.

Capítulo 5. Seguridad

1. Introducción

Para la implementación y lanzamiento de los sorteos electrónicos de LOTENAL, uno de los requerimientos específicos hacia la Dirección de Servicios Informáticos fue la de minimizar los riesgos de seguridad en el proyecto, de manera que éste contara con un esquema de seguridad que permitiera la evaluación del entorno y desarrollo del mismo.

En este capítulo revisaremos el esquema de seguridad utilizado en Loterías Electrónicas, no solamente en la implementación de los algoritmos, sino también en la arquitectura e infraestructura del proyecto en general. Comenzamos al igual que en los capítulos anteriores, mencionando algunas definiciones importantes para la comprensión de este tema.

1.1 Criptología (Criptografía y Criptoanálisis)

La criptología (del griego *criptos*=oculto y *logos*=tratado, ciencia) es el nombre genérico con el que se designan dos disciplinas opuestas y a la vez complementarias: criptografía y criptoanálisis. La criptografía se ocupa del diseño de procedimientos para cifrar, es decir, para enmascarar una determinada información de carácter confidencial. El criptoanálisis, por su parte, se ocupa de romper esos procedimientos de cifrado para así recuperar la información original. Ambas disciplinas siempre se han desarrollado de forma paralela, pues cualquier método de cifrado lleva siempre emparejado su criptoanálisis correspondiente.

La criptografía como medio de proteger la información personal es un arte tan antiguo como la propia escritura. Como tal, permaneció durante siglos vinculada muy estrechamente a los círculos militares y diplomáticos, puesto que eran los únicos que en principio tenían auténtica necesidad de ella.

En la actualidad la situación ha cambiado drásticamente: el desarrollo de las comunicaciones electrónicas unido al uso masivo y generalizado de las computadoras, hace posible la transmisión y almacenamiento de grandes flujos de información confidencial que es necesario proteger. Es entonces cuando la criptografía pasa de ser exigencia de minorías a convertirse en una necesidad real del hombre común que ve en esta falta de protección de sus datos privados una amenaza para su propia intimidad.

A continuación se muestra el esquema fundamental de un proceso criptográfico (cifrado/descifrado)

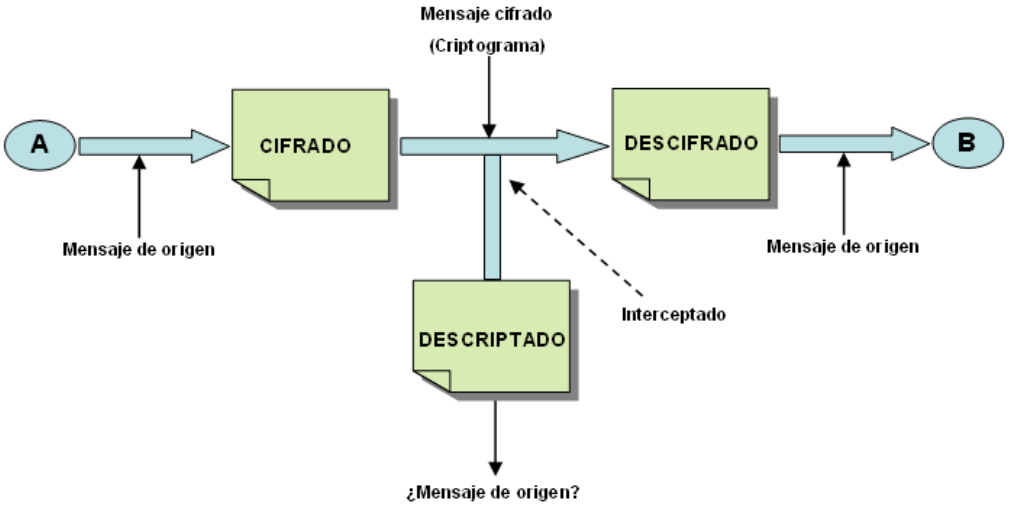


Figura 5.1 Proceso general cifrado/descifrado

A y B son, respectivamente, el emisor y receptor de un determinado mensaje. A transforma el mensaje original (texto claro o texto fuente), mediante un determinado procedimiento de cifrado

controlado por una clave, en un mensaje cifrado (criptograma) que se envía por un canal público. En recepción, B con conocimiento de la clave transforma ese criptograma en el texto fuente recuperando así la información original.

En el proceso de transmisión, el criptograma puede ser interceptado por un enemigo criptoanalista que lleva a cabo una labor de descriptado; es decir, intenta, a partir del criptograma y sin conocimiento de la clave, recuperar el mensaje original. Un buen sistema criptográfico será, por tanto, aquel que ofrezca un descifrado sencillo pero un descriptado imposible o, en su defecto, muy difícil.

1.2 Objetivos de la Criptografía

Los objetivos de la criptografía son múltiples: primeramente, mantener la confidencialidad del mensaje; es decir, que la información allí contenida permanezca secreta; a continuación, garantizar la autenticidad tanto del criptograma (integridad) como del par remitente/destinatario. En efecto, el criptograma recibido ha de ser realmente el enviado (evitando así manipulaciones o alteraciones en el proceso de transmisión), a la vez que el remitente y destinatario han de ser realmente quienes dicen ser, y no remitentes y/o destinatarios fraudulentos. La criptografía clásica se ocupaba únicamente del primer aspecto, mientras que la criptografía de hoy en día, basada en el concepto de comunicaciones seguras, ha de garantizar conjuntamente todas ellas.

1.3 Algoritmo Criptográfico

Un algoritmo criptográfico, o cifrador, es una función matemática usada en los procesos de cifrado y descifrado. Un algoritmo criptográfico trabaja en combinación con una llave (un número, palabra, frase, o contraseña) para cifrar y descifrar datos. Para cifrar, el algoritmo combina matemáticamente la información a proteger con una llave provista. El resultado de este cálculo son los datos cifrados. Para descifrar, el algoritmo hace un cálculo combinando los datos cifrados con una llave provista, siendo el resultado de esta combinación los datos descifrados (exactamente igual a como estaban antes de ser cifrados). Si la llave o los datos son modificados el algoritmo produce un resultado diferente.

El tipo particular de transformación aplicada al texto claro (mensaje sin cifrar) o las características de las claves utilizadas marcan la diferencia entre los diversos métodos criptográficos. Una primera clasificación en base a las claves utilizadas es la siguiente:

1.3.1 Algoritmos Simétricos

Son aquéllos en los que la clave de cifrado coincide con la de descifrado. Lógicamente, dicha clave tiene que permanecer secreta, lo que presupone que emisor y receptor se han puesto de acuerdo previamente en la determinación de la misma, o bien que existe un centro de distribución de claves que se la han hecho llegar a ambos por un canal seguro.

Algunos ejemplos de algoritmos simétricos son DES, 3DES, RC5, AES, Blowfish e IDEA.

1.3.1.1 Cifrado DES

En 1973, el NBS (Nacional Bureau of Standard, USA) organizó un concurso solicitando un algoritmo de encriptación para la protección de datos de una computadora durante su transmisión y almacenaje. En 1974, la corporación IBM presentó, entre otras, una propuesta, inspirada en sus sistema propietario LICIFER, que, convenientemente modificada, dio lugar al Data Encryption Standard (Norma de encriptación de datos), abreviadamente llamado DES. La aprobación y modificación de la propuesta se hizo bajo la supervisión de la NSA (Nacional Security Agency, USA).

No obstante, la NSA fue la que impuso la longitud de clave del DES, que es bastante modesta y que la hace desaconsejable con el actual desarrollo de la informática.

El DES es un algoritmo de cifrado en bloque[14]; la longitud de bloque es de 64 bits (ocho símbolos ASCII); la longitud de la clave es de 56 bits, lo que equivale a que existan 2^{56} = 7,2*10^{16} claves diferentes.

1.3.1.2 Estructura del DES

El algoritmo DES funciona de la siguiente manera: Se hace una permutación inicial fija del bloque a cifrar, y, por tanto, sin valor criptográfico. Después se divide el bloque en dos mitades, la derecha y la izquierda. A continuación se realiza una operación modular que se repite 16 veces; esta operación consiste en sumar módulo 2 la parte izquierda con una función $F(K_i)$ de la parte derecha, gobernada por una clave K_i. Después se intercambian las partes derecha e izquierda. En la figura 1 se representa el esquema. En la vuelta número 16 se omite el intercambio, pero se remata el algoritmo con una permutación final que es la inversa de la inicial.

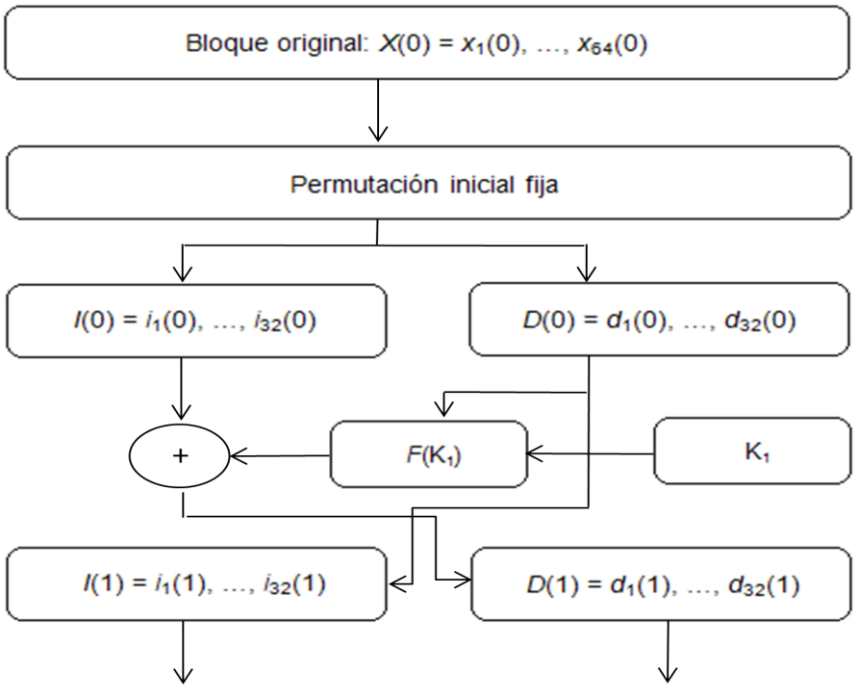


Figura 5.2 Estructura del DES

1.3.1.3 Cifrado 3DES

Se le llama así al algoritmo que hace triple cifrado del DES. También es conocido como TDES, fue desarrollado por IBM en 1998.

Cuando se descubrió que una clave de 56 bits no era suficiente para evitar un ataque de fuerza bruta, TDES fue elegido como forma de agrandar el largo de la clave sin necesidad de cambiar de algoritmo de cifrado. Este método de cifrado es inmune al ataque por encuentro a medio camino, doblando la longitud efectiva de la clave (112 bits), pero en cambio es preciso triplicar el número de operaciones de cifrado, haciendo este método de cifrado muchísimo más seguro que el DES.

El Triple DES está desapareciendo lentamente, siendo reemplazado por el algoritmo AES. Sin embargo, la mayoría de las tarjetas de crédito y otros medios de pago electrónicos tienen como estándar el algoritmo Triple DES (anteriormente usaban el DES). Por su diseño, el DES y por lo tanto el TDES son algoritmos lentos. AES puede llegar a ser hasta 6 veces más rápido y a la fecha no se ha encontrado ninguna vulnerabilidad.

[14] Se denomina cifrado en bloque aquel en el que se cifra el mensaje original agrupando los símbolos en grupo (bloques) de dos o más elementos. Algunos sistemas de cifrado en bloque son el poligráfico y el de transposición.

1.3.1.4 Ventajas y Desventajas de la Criptografía Simétrica

El principal problema con los sistemas de cifrado simétrico no está ligado a su seguridad, sino al intercambio de claves. Una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad, pero ¿qué canal de comunicación que sea seguro han usado para transmitirse las claves? Tal vez sería mucho más fácil para un atacante intentar interceptar una clave que probar las posibles combinaciones del espacio de claves.

Otro problema es el número de claves que se necesitan. Si tenemos un número n de personas que necesitan comunicarse entre sí, se necesitan n/2 claves para cada pareja de personas que tengan que comunicarse de modo privado. Esto puede funcionar con un grupo reducido de personas, pero sería imposible llevarlo a cabo con grupos más grandes. Su principal ventaja es su velocidad.

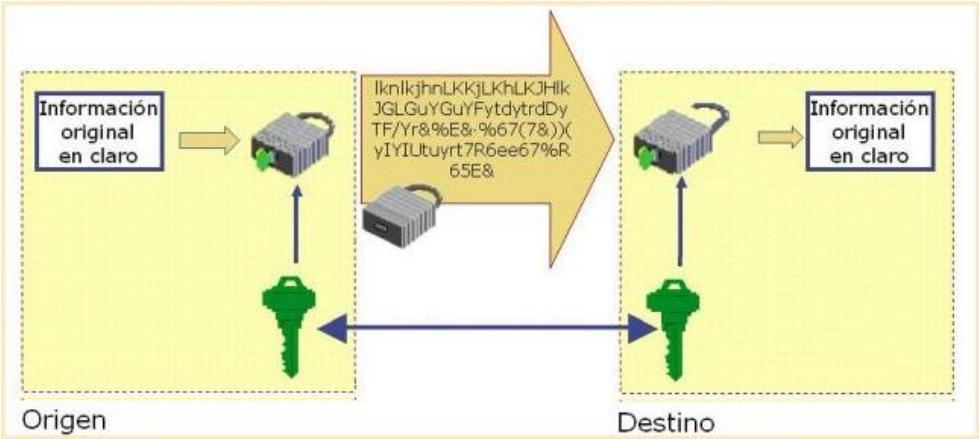


Figura 5.3 Cifrado Simétrico
(Ventaja: Velocidad)

1.3.2 Algoritmos Asimétricos

Son aquellos en los que la clave de cifrado es diferente a la de descifrado. En general, la clave de cifrado es conocida libremente por el público, mientras que la de descifrado es conocida únicamente por el usuario.

Algunos ejemplos de algoritmos asimétricos son RSA, ElGamal, Curvas Elípticas.

1.3.2.1 Ventajas y Desventajas de la Criptografía Asimétrica

Los algoritmos asimétricos necesitan al menos una llave de 3000 bits para alcanzar un nivel de seguridad similar al de uno simétrico de 128 bits, y son increíblemente lentos, tanto que no pueden ser utilizados para cifrar grandes cantidades de información. Los algoritmos simétricos son aproximadamente 1000 veces más rápidos que los asimétricos. Su principal ventaja es el uso de diferentes claves para cifrar y descifrar, lo que le da a la clave cierta confidencialidad.

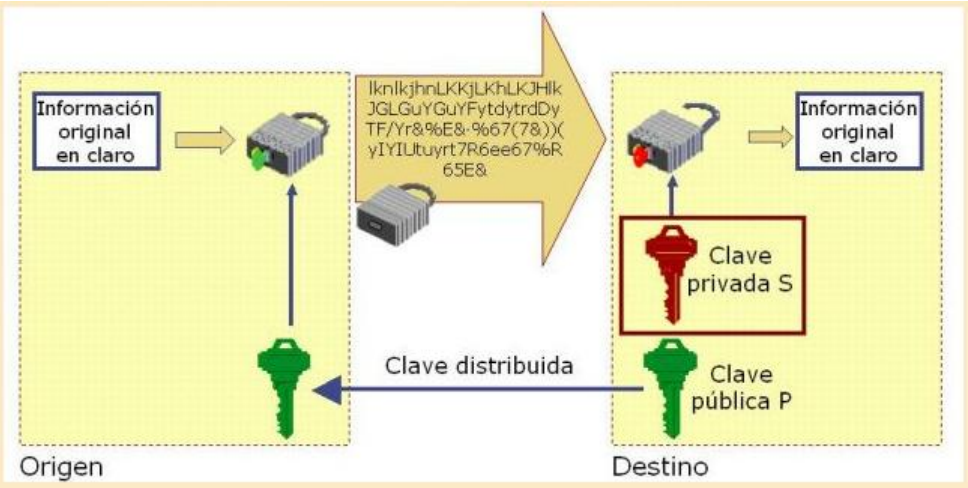


Figura 5.4 Cifrado Asimétrico
(Ventaja: Confidencialidad)

Los métodos simétricos son propios de la *criptografía clásica* o c*riptografía de clave secreta*, mientras que los métodos asimétricos corresponden a la c*riptografía de clave pública*, introducida por Diffie y Hellman[15] en 1976.

1.4 Seguridad Criptográfica

Una de las diferencias fundamentales entre la criptografía clásica y la criptografía de hoy en día radica en el concepto de "seguridad". Antes, los procedimientos de cifrado tenían una seguridad probable; hoy, los procedimientos de cifrado han de tener una seguridad matemáticamente demostrable. Esto lleva a la siguiente clasificación de seguridad criptográfica:

- Seguridad incondicional (teórica): El sistema es seguro frente a un atacante con tiempo y recursos computacionales ilimitados. Ejemplo: cifrado Vernam.

- Seguridad computacional (práctica): El sistema es seguro frente a un atacante con tiempo y recursos computacionales limitados. Ejemplo: sistemas de clave pública basados en problemas de alta complejidad de cálculo.

- Seguridad probable: No se puede demostrar su integridad, pero el sistema no ha sido violado. Ejemplo: cifrado DES.

- Seguridad condicional: Todos los demás sistemas, en tanto que el enemigo carece de medios para atacarlos.

Con los antiguos procedimientos manuales y lentos de criptoanálisis era suficiente la seguridad condicional, pues en la mayoría de los casos el descriptado del mensaje se obtenía cuando la información del documento había perdido toda validez. Si el criptoanálisis tuvo éxitos de importancia fue solo porque, al igual que era lento el proceso de análisis, lo era también el de cambio de claves. En la actualidad, con el uso de potentes computadoras para el criptoanálisis, los algoritmos criptográficos tienen que tener propiedades matemáticas que los hagan invulnerables no sólo en el presente, sino también en un futuro, a corto y mediano plazo.

Ahora que ya conocemos conceptos teóricos de criptografía, analizaremos el esquema de seguridad utilizado en el proyecto de Loterías electrónicas.

[15] Diffie, W., y Hellman, M. E., "New directions in cryptography", IEEE Transactions of Information Theory, IT-22 (1976, 644-654)

2. Esquema de Seguridad Loterías Electrónicas

Recordemos que las transacciones realizadas en los sorteos electrónicos, se efectúan en tiempo real, por lo tanto el software debería reforzar los siguientes puntos de vulnerabilidad:

1. Debido a que la Base de Datos de Premios se genera en tiempo real, durante la celebración del Protocolo de Inicio de Sorteos en LOTENAL (Sembrado de Premios), la información que ésta contiene (billetes y premios asociados) no debe ser almacenada en claro, puesto que cualquier persona podría verificar cuál es el billete con el premio mayor asignado.

2. Al momento de que las Loterías Electrónicas respondan a una solicitud, sobre todo de validación de premios, como dicha respuesta es entregada al Distribuidor (DATANET) y enviada de éste hacia la Institución Bancaria mediante internet, la información que viaja a través del canal de comunicación es susceptible de ataques.

3. El servidor de peticiones implementado en las Loterías Electrónicas debe cerciorarse sobre la identidad del cliente que le solicita el servicio (el cual únicamente debe ser el cliente instalado en DATANET) y así, evitar el responder a solicitudes de intrusos.

4. Una vez generada e instalada la Base de Datos de premios del sorteo electrónico es vulnerable a accesos de intrusos que pretendan conseguir la clave de cifrado de información y con ella conocer el número de billete ganador del premio mayor.

Para atacar estos puntos de vulnerabilidad detectados en el proyecto se tomaron respectivamente las siguientes acciones:

1. Cifrar la Base de Datos de Premios con algoritmo 3DES.
2. Cifrar la cadena de información de la transacción que viaja a DATANET mediante un algoritmo DES (cifrado en el medio).
3. Utilizar como canal de comunicación entre el servidor de peticiones de LOTENAL y DATANET una VPN dedicada.
4. Proteger el servidor (computadora) en el cual radique la Base de Datos de Premios con un software de control de accesos robusto basado en un esquema de privilegios en base a roles y perfiles de usuario.

2.1 Base de Datos de Premios Cifrada con Algoritmo 3DES

El objetivo de un algoritmo criptográfico es hacer tan difícil como sea posible descifrar los datos sin utilizar la clave. Si se usa un algoritmo de encriptación realmente bueno, entonces no hay ninguna técnica significativamente mejor que intentar metódicamente con cada clave posible. Incluso para una clave de sólo 40 bits, esto significa 2ˆ40 (poco más de 1 trillón) de claves posibles.

Actualmente, las computadoras pueden descifrar claves con extrema rapidez, y ésta es la razón por la cual el tamaño de la llave es importante en los criptosistemas modernos. Como se mostró anteriormente el algoritmo de cifrado DES usa una clave de 56 bits, lo que significa que hay 2ˆ56 claves posibles (72.057.594.037.927.936 claves). Esto representa un número muy alto de claves, pero una computadora ordinaria puede comprobar el conjunto posible de claves en cuestión de días. Una máquina especializada puede hacerlo en horas.

Por esta razón se consideró utilizar una clave más fuerte en cuestiones de seguridad para proteger la información de la Base de Datos de los premios, y se optó por utilizar el algoritmo de cifrado 3DES con una llave de 112 bits, lo que significa que existen 2ˆ112 claves posibles de cifrado de datos.

La clave 3DES es única por sorteo, y se genera aleatoriamente durante el Protocolo de Inicio de Sorteos en LOTENAL (Sembrado de Premios). Con ella se cifra información sensible tal como el monto del premio asociado al billete participante.

Una de las desventajas observadas en este proceso es la lentitud. El cifrado de la información utilizando una clave 3DES es mucho más lento que el DES, y en la experiencia de la propia Institución, hablando de sorteos con una emisión total de 2,500,000 billetes electrónicos, llegaba a tardarse hasta 6 horas.

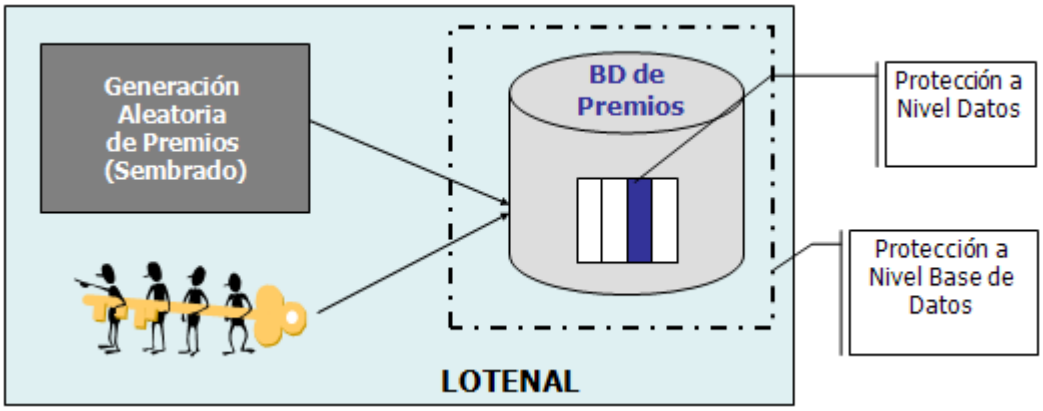


Figura 5.5 Base de Datos de Premios cifrada en 3DES

2.2 Cifrado en el Medio DES

La respuesta a solicitudes de generación de números participantes y venta de billetes electrónicos es entregada por el servidor de peticiones de LOTENAL a DATANET como un mensaje cifrado en DES. Si bien es cierto que el algoritmo DES resulta más vulnerable a ataques que el 3DES, los motivos por los cuales fue seleccionado en su momento como algoritmo de cifrado en el medio fueron los siguientes:

- Compatibilidad Bancaria: HSBC manejaba como estándar interno este algoritmo, lo cual agilizó tiempo ya que el Área Informática del Banco no tuvo necesidad de implementar un nuevo algoritmo.

- Rapidez: Para transacciones de respuesta al usuario en tiempo real, se necesitaba un algoritmo que fuera rápido y los procesos de cifrado y descifrado 3DES gastaban más tiempo.

Recordemos además que una respuesta a solicitud de números participantes y validación de premios es una transacción realizada, si se intentara descriptar el criptograma se obtendrían ya sea los billetes electrónicos participantes en la oportunidad de juego o el resultado del premio correspondiente a un billete seleccionado que en su caso ya se considera vendido. Esta información es importante pero poco sensible porque no aporta datos que pudieran servir para conocer el billete ganador de un premio o la clave de cifrado 3DES, de hecho, la clave de cifrado en el medio no tiene nada que ver con la clave de cifrado de la Base de Datos de Premios del Sorteo.

La clave DES también se genera durante el Protocolo de Inicio de Sorteos en LOTENAL (Sembrado de Premios), siendo aleatoria y única por sorteo. Como ya lo mencionamos anteriormente, durante este proceso se reúnen físicamente en las instalaciones del centro de cómputo de LOTENAL las autoridades responsables de la generación del sorteo y un interventor de la Secretaría de Gobernación.

Frente al interventor de la Secretaría de Gobernación el sistema imprime la llave de cifrado DES generada, la cual también es dada de alta en los sistemas de información de DATANET, ya que, como se mencionó anteriormente, el algoritmo DES es simétrico, lo cual implica el conocimiento de la llave por parte de LOTENAL (cifrar la cadena de datos) y por parte de DATANET (decifrar la cadena de datos)

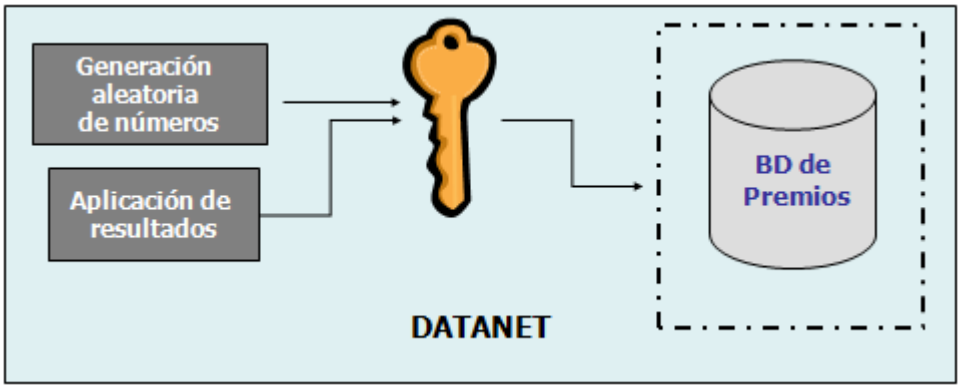


Figura 5.6 Procesos de descifrado 3DES

2.3 VPN dedicada

Una VPN en IP es una conexión privada entre dos o más computadoras que intercambian tráfico privado a través de una red pública compartida como internet (enlaces de banda ancha ADSL). Esta tecnología permite a las organizaciones extender sus servicios de red, a través de Internet, hacia sus sucursales y usuarios remotos creando una WAN (Wide Area Network) privada vía Internet.

Utilizando tunneling[16], encriptación, autenticación y tecnología de directorios, las Redes Privadas Virtuales en IP ofrecen confidencialidad y el más alto nivel de seguridad en el intercambio de datos de la Institución, además de ahorros considerables en los gastos de operación.

En LOTENAL se implementó una VPN entre el servidor de loterías electrónicas y el servidor de DATANET encargado de hacer las peticiones de generación de números aleatorios y validación de premios.

La VPN provista por LOTENAL incluye dentro de sus soluciones medidas de seguridad tales como cifrado de la información que viaja por el túnel de comunicación, autenticación de usuarios, firewalls[17] y antivirus de chequeo para contrarrestar los diferentes tipos de amenazas a la seguridad de la red.

2.3.1 ¿Cómo trabaja una VPN?

En una VPN la Institución utiliza su ancho de banda de Internet para establecer conexiones privadas y seguras entre sus empleados y oficinas remotas. Cada usuario remoto se conecta con el proveedor de servicio de Internet local en la misma forma que accesa a Internet por marcado telefónico, cable, DSL, ISDN, T1, wireless, etc.

Un proceso llamado “túnel” es usado para llevar la información sobre Internet. Para asegurar una transmisión del túnel contra intercepciones, todo el tráfico sobre la VPN es encriptado para su seguridad.

Esencialmente hacer un túnel es el proceso de colocar todo un paquete dentro de otro (el cual proporciona información de ruteo) y enviarlo sobre Internet. La ruta a través de la cual los paquetes viajan es llamada túnel. Para que un túnel sea establecido, el túnel del servidor y del cliente debe estar usando el mismo protocolo de túnel.

Dos protocolos populares para hacer túnel son los siguientes:

[16] La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras.
[17] Cortafuegos o Firewall es un elemento de software y/o hardware diseñado para bloquear el acceso no autorizado a una fuente de datos, y al mismo tiempo permitir aquellos que sí lo están.

- PPTP: Protocolo de Túnel Punto a Punto (Point-to-Point Tunneling Protocol)
- IPSec: Protocolo de Seguridad de Internet (Internet Protocol Security)

La ventaja de IPSec es que provee mejor seguridad, con un cifrado más fuerte y de más alto desempeño que PPTP.

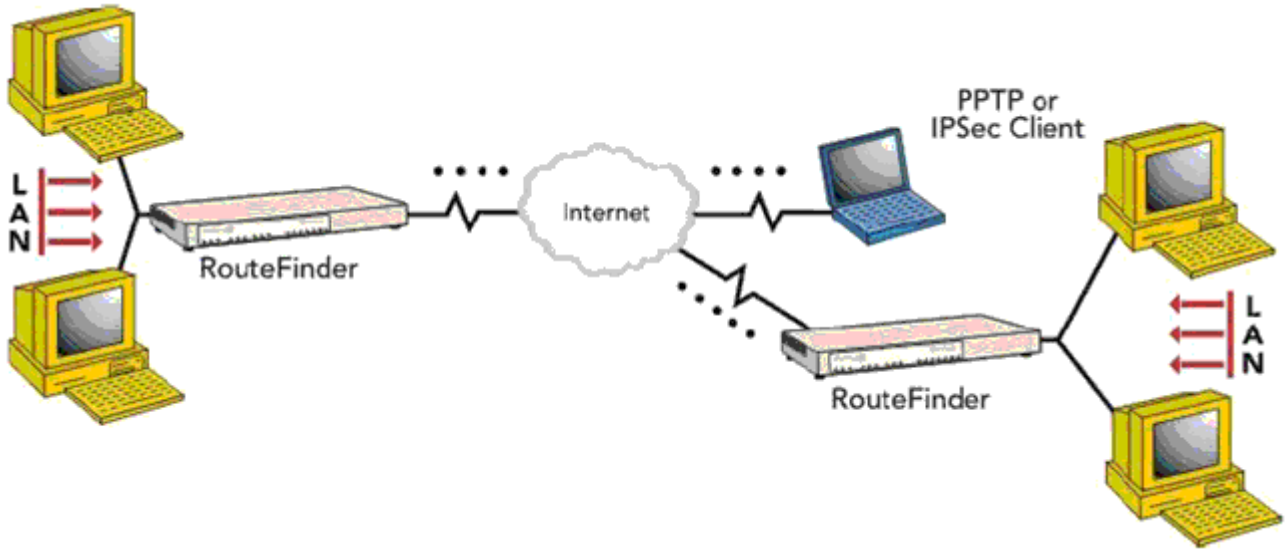


Figura 5.7 Red Privada Virtual (VPN)

2.4 Control de Accesos

El temor principal de un ataque al sorteo electrónico radica en corromper la integridad de la Base de Datos de Premios. El sistema de Loterías Electrónicas mediante las Aplicaciones de Protocolos de Cierre de Sorteos realiza procesos que permiten conciliar la información final de las ventas reportadas contra la base de premios original generada para el sorteo. Estos procesos permiten al final de la vida del sorteo saber si éste fue “limpio”, sin embargo se necesita proteger la información a un nivel de control de accesos al servidor que aloja la Base de Datos de Premios del Sorteo y al servidor sobre el cual se instale la aplicación de Loterías Electrónicas.

Para tal efecto, se instaló en LOTENAL y en DATANET el software de Control de Accesos Entrust con las siguientes características:

- Instalación del servidor
- Servidor PKI[18] y Unidad Certificadora (CA)
- Interfaz Administrativa
- Interfaz de Configuración
- API y Manual del API para la integración del desarrollo del producto
- Generador de llaves (pública y privada)
- Generador de Certificados Digitales
- Script de instalación
- Privilegios de acceso a usuarios basados en roles y perfiles
- Bitácoras de accesos

[18] **Public Key Infrastructure**, Infraestructura de Llave Pública es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

Este software permite tener control y registro de todas las personas o aplicaciones que acceden al servidor, y con las bitácoras y herramientas que proporciona se pueden generar reportes y artefactos auditables que permiten identificar acciones dolosas.

En un inicio del proyecto se consideró generar las llaves de cifrado DES y 3DES a partir de certificados digitales proporcionados por la Unidad Certificadora de Entrust, sin embargo esa funcionalidad se definió para siguientes fases del Proyecto.

3. WLA (World Lottery Association)

Para las compañías de lotería, la confianza es esencial. La seguridad es crucial y aumenta la necesidad de demostrar que los procesos internos están a la altura de las mejores prácticas sectoriales. Operaciones de lotería deshonestas de parte de compañías nada serias desgastan la confianza del público, lo que perjudica el sector regulado del juego.

Independientemente de su tamaño, las loterías hacen frente a exigencias de seguridad de diversas partes interesadas. A raíz de la desregulación y la penetración de Internet, los fraudes de lotería por parte de actores nada serios predominan cada vez más.

El organismo World Lottery Association (WLA, por sus siglas en inglés) trabaja para proteger la integridad y promover el rol de las loterías con concesiones estatales en calidad de generadoras de fondos para buenas causas. Al centrarse en los sistemas de seguridad, WLA desea subrayar la importancia de la seguridad y la visibilidad de los procedimientos en las operaciones de lotería.

WLA ha desarrollado las normas WLA Security Control Standards, que son estándares de seguridad adaptados a la medida de las operaciones de lotería.

Para una institución como LOTENAL, la certificación de sus operaciones según esta norma demuestra que el sistema de seguridad de su lotería está a la altura de buenas prácticas en el sector de juegos. El sistema de Loterías Electrónicas cumple Las Normas de Control de Seguridad de la WLA

Conclusiones

Sabemos que la tecnología está en constante evolución, y cada vez nuevas y mejores herramientas salen al mercado para optimizar y facilitar el desarrollo de sistemas. Cada empresa deberá realizar las labores de mantenimiento y reingeniería necesarias para ajustarse a los cambios que demanda este crecimiento vertiginoso de sistemas de información.

Aún con todo esto, el Proyecto de Loterías Electrónicas para LOTENAL fue muy importante porque revolucionó el concepto de los sorteos tradicionales de la Institución. Su arquitectura permitió extender los puntos de venta no solamente a Cajeros Automáticos, de tal forma que hoy día LOTENAL tiene el mismo producto en diversos canales de comercialización tales como:

1. Lotería Electrónica Soriana: Venta mediante Cajas Registradoras de Soriana
2. Cachito Móvil: Venta mediante telefonía móvil
3. Cachito Móvil (Internet): Venta mediante internet

A partir de las Loterías electrónicas en LOTENAL surgieron diferentes iniciativas de sorteos que actualmente están a la venta y podemos encontrar en el mercado de Azar.

Anexo

1. Prueba de Kolmogorov–Smirnov para dos muestras del mismo tamaño

	$1-\alpha$				
n	0.80	0.90	0.95	0.98	0..99
3	2	2			
4	3	3	3		
5	3	3	4	4	4
6	3	4	4	5	5
7	4	4	5	5	5
8	4	4	5	5	6
9	4	5	5	6	6
10	4	5	6	6	7
11	5	5	6	7	7
12	5	5	6	7	7
13	5	6	6	7	8
14	5	6	7	7	8
15	5	6	7	8	8
16	6	6	7	8	9
17	6	7	7	8	9
18	6	7	8	9	9
19	6	7	8	9	9
20	6	7	8	9	10
21	6	7	8	9	10
22	7	8	8	10	10
23	7	8	9	10	10
24	7	8	9	10	11
25	7	8	9	10	11
26	7	8	9	10	11
27	7	8	9	11	11
28	8	9	10	11	11
29	8	9	10	11	12
30	8	9	10	11	12
31	8	9	10	11	12
32	8	9	10	12	12
33	8	9	10	12	12
34	8	10	11	12	13
35	8	10	11	12	13
36	9	10	11	12	13
37	9	10	11	Í2	13
38	9	10	11	13	14
39	9	10	12	13	14
40	9	10	12	13	14
$n > 40$	$1.52/\sqrt{n}$	$1.73/\sqrt{n}$	$1.92/\sqrt{n}$	$2.15/\sqrt{n}$	$2.30/\sqrt{n}$

2. Prueba de Kolmogorov–Smirnov para dos muestras de diferente tamaño

		$1-\alpha$				
n_1	n_2	0.80	0.90	0.95	0.98	0.99
1	9	17/18				
	10	9/10				
2	3	5/6				
	4	3/4				
	5	4/5	4/5			
	6	5/6	5/6			
	7	5/7	6/7			
	8	3/4	7/8	7/8		
	9	7/9	8/9	8/9		
	10	7/10	4/5	9/10		
3	4	3/4	3/4			
	5	2/3	4/5	4/5		
	6	2/3	2/3	5/6		
	7	2/3	5/7	6/7	6/7	
	8	5/8	3/4	3/4	7/8	
	9	2/3	2/3	7/9	8/9	8/9
	10	3/5	7/10	4/5	9/10	9/10
	12	7/12	2/3	3/4	5/6	11/12
4	5	3/5	1/4	4/5	4/5	
	6	7/12	2/3	3/4	5/6	5/6
	7	17/28	5/7	1/4	6/7	6/7
	8	5/8	5/8	3/4	7/8	7/8
	9	5/9	2/3	3/4	7/9	8/9
	10	11/20	13/20	7/10	4/5	4/5
	12	7/12	2/3	2/3	1/4	5/6
	16	9/16	5/8	Í1/16	1/4	13/16
5	6	1/5	2/3	2/3	5/6	5/6
	7	4/7	23/25	5/7	29/15	6/7
	8	11/20	5/8	27/40	4/5	4/5
	9	5/9	3/5	31/45	7/9	4/5
	10	1/2	3/5	7/10	7/10	4/5
	15	8/15	3/5	2/3	11/15	11/15
	20	1/2	11/20	3/5	7/10	3/4
6	7	23/42	4/7	29/42	5/7	5/6
	8	1/2	7/12	2/3	3/4	3/4
	9	1/2	5/9	2/3	13/18	7/9
	10	1/2	17/30	19/10	7/10	11/45
	12	1/2	7/12	7/12	2/3	3/4
	18	4/9	5/9	11/18	2/3	13/18
	24	11/24	1/2	7/12	5/8	2/3
7	8	27/56	33/56	5/8	41/56	3/4
	9	31/63	5/9	40/63	5/7	47/63
	10	13/70	39/70	43/70	7/10	5/7
	14	3/7	1/2	4/7	9/14	5/7
	28	3/7	13/28	15/28	17/28	9/14

		$1-\alpha$				
n_1	n_2	0.80	0.90	0.95	0.98	0.99
8	8	4/9	13/24	5/8	2/3	3/4
	10	19/40	21/40	21/40	27/40	7/10
	12	11/24	1/2	7/12	5/8	2/3
	16	7/16	1/2	9/16	5/8	5/8
	32	13/32	7/16	1/2	9/16	19/32
9	10	7/15	1/2	26/45	2/3	31/45
	12	4/9	1/2	5/9	11/18	2/3
	15	19/45	22/45	8/15	3/5	29/45
	18	7/18	4/9	1/2	5/9	11/18
	36	13/36	5/12	17/36	19/36	5/9
10	15	2/5	7/15	1/2	17/30	19/30
	20	2/5	9/20	1/2	11/20	3/5
	40	7/20	2/5	9/20	1/2	
12	15	23/60	9/20	1/2	11/20	7/12
	16	3/8	7/16	23/48	13/24	7/12
	18	13/36	5/12	17/36	19/36	5/9
	20	11/30	5/12	7/15	31/60	17/30
15	20	7/20	2/5	13/30	29/60	31/60
16	20	27/80	31/80	17/40	19/40	41/80
		$1.07\sqrt{\frac{n_1+n_2}{n_1 \cdot n_2}}$	$1.22\sqrt{\frac{n_1+n_2}{n_1 \cdot n_2}}$	$1.36\sqrt{\frac{n_1+n_2}{n_1 \cdot n_2}}$	$1.48\sqrt{\frac{n_1+n_2}{n_1 \cdot n_2}}$	$1.63\sqrt{\frac{n_1+n_2}{n_1 \cdot n_2}}$

Glosario de Términos

- **API:** (Application Programming Interface) es el conjunto de funciones y procedimientos (o métodos, en la programación orientada a objetos) que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción. Son usadas generalmente en las bibliotecas (también denominadas comúnmente "librerías").

- **ATM:** Siglas en ingles de un Cajero Automático (Automated Teller Machine)

- **DES:** (Data Encryption Standard), es un algoritmo de cifrado, es decir, un método para cifrar información, escogido como FIPS en los Estados Unidos en 1976, y cuyo uso se ha propagado ampliamente por todo el mundo.

- **FIPS:** (Federal Information Processing Standard). Es una publicación de estándares federales de procesamiento de la información de los Estados Unidos, para la acreditación de módulos criptográficos. La serie de publicaciones FIPS se emitió para coordinar los requerimientos y estandarización de módulos criptográficos en los que incluye componentes hardware y software.

- **Investigación Causal:** Un tipo de investigación que tiene hipótesis muy específicas y que se diseña generalmente para proporcionar el nivel fundamental de comprensión – un conocimiento de que una variable, en ciertas condiciones, hace que ocurra o cambie otra variable.

- **Investigación Descriptiva:** Información que se diseña para proporcionar un resumen de algunos aspectos del entorno cuando las hipótesis son tentativas y especulativas por naturaleza.

- **Investigación Exploratoria:** Método de investigación que se diseña generalmente para generar ideas cuando las hipótesis son vagas o están mal definidas.

- **ISO 9000:** Conjunto de normas sobre calidad y gestión continua de calidad, establecidas por la Organización Internacional de Normalización (ISO). Se pueden aplicar en cualquier tipo de organización o actividad orientada a la producción de bienes o servicios. El ISO 9000 especifica la manera en que una organización opera, sus estándares de calidad, tiempos de entrega y niveles de servicio.

- **J2SE:** (Java Platform, Standard Edition o Java SE, conocido anteriormente hasta la versión 5.0 como Plataforma Java 2, Standard Edition o J2SE), es una colección de APIs del lenguaje de programación Java útiles para muchos programas de la Plataforma Java.

- **LOTENAL:** Lotería Nacional para la Asistencia Pública

- **NSE:** Nivel Socioeconómico

- **Número Pseudos-aleatorio:** Es un número generado en un proceso que parece producir números al azar, pero no lo hace realmente. Las secuencias de números pseudo-aleatorios no muestran ningún patrón o regularidad aparente desde un punto de vista estadístico, a pesar de haber sido generadas por un algoritmo completamente determinista, en el que las mismas condiciones iniciales producen siempre el mismo resultado. Los mecanismos de generación de números aleatorios que se utilizan en la mayoría de los sistemas informáticos son en realidad procesos pseudo-aleatorios.

- **PKI:** (Public Key Infrastructure) Infraestructura de Llave Pública es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

- **SEGOB:** Decretaría de Gobernación

- **TI:** Tecnología de Información

- **Triple DES:** En criptografía Triple DES (3DES) se llama al algoritmo que hace triple cifrado del DES. También es conocido como TDES o 3DES, fue desarrollado por IBM en 1978.

Índice de Tablas y Gráficas

Bibliografía

“Investigación de Mercados”
David A. Aaker, V. Kumar, George S. Day
Editorial Limusa, 2001

“Técnicas Criptográficas de protección de datos”
Amparo Fúster Sabater, Dolores de la Guía Hernández, Luis Hernández Encinas, Fausto Montoya Vitinil, Jaime Muñoz Masqué
Editorial Ra – Ma, 2000

“Historia de la Lotería Nacional para la Asistencia Pública”
Marcela Estrada Attolinl, Heidy Basave Ochoa
Editorial Creatividad Tipográfica S. A. 1981