La seguridad del programa de resultados electorales preliminares

El problema de la seguridad en el PREP 97 presentó, desde el principio, un alto grado de complejidad dado que eran muchos aspectos los que debían considerarse, además de que se heredaba, de ocasiones anteriores, un temor generalizado por la posibilidad de que fuera objeto de atentados. Por un lado, se tenía la premisa de garantizar la absoluta transparencia en todo el proceso a fin de lograr credibilidad en los comicios y, por otro, la necesidad de prevenir cualquier tipo de contingencia y brindar total protección contra los posibles atacantes. Esto hizo que la tarea fuese doblemente difícil.

El Dr. Enrique Daltabuit Godas, Asesor en Seguridad, explica que la seguridad era necesaria por tres razones principales:

"Una es de tipo histórico, había que evitar que sucediera algún incidente de negación de servicio como en las elecciones pasadas cuando causó alboroto a nivel político y en la comunidad informática en México.

"En segundo lugar, la razón obvia de implantar cualquier sistema de seguridad es garantizar la preservación de los datos que forman parte de un sistema de información. En cualquier sistema de información hay una serie de normas que hay que seguir para preservar los datos; estas tienen que ver con su integridad, con su confiabilidad, con una serie de especificaciones técnicas que son ampliamente conocidas por quien se dedica a la seguridad. Cualquier sistema de información que no incorpore estos parámetros en su diseño, esta mal diseñado, es mala ingeniería, es inaceptable en el mundo moderno.

"La tercera, que puede ser el corolario o el preludio de este diseño y que es uno de los principios básicos de la seguridad, es el que

llaman el principio de la proporcionalidad. El esfuerzo que se haga en seguridad de un sistema de información debe ser adecuado al valor y a la importancia de los datos que se estén protegiendo. En el caso de un sistema electoral como el que se maneja en México, el valor de esta información es prácticamente ilimitado, entonces el esfuerzo de seguridad que hay que hacer es intenso, es necesario y es inevitable. Esto no quiere decir que tenga que ser necesariamente muy caro, pero es algo que no se puede soslayar."

Al definirse la estrategia general del Programa, se determinó un objetivo general de seguridad informática que consistió en asegurar que la información contenida en las actas recibidas en los CEDAT coincidiera exactamente con la información publicada. Esta seguridad se tuvo que dar en un contexto de múltiples atacantes potenciales, algunos de ellos con amplios recursos técnicos y económicos. Podría haber existido alguien interesado en hacer fracasar el PREP ya que, en la medida en la que constituía una garantía de legalidad y transparencia de las elecciones, quien quisiera basar su estrategia política en la denuncia o descalificación del proceso electoral encontraría en el PREP un obstáculo. Por otra parte, dado el poco tiempo de que se dispuso para la presentación de los resultados, los numerosos puntos de captura y la gran cantidad de personas que participaron, las probabilidades de error eran altas.

También fue necesario un estricto control de las personas que tenían acceso al centro de cómputo debido a la naturaleza de las actividades que en él se realizaban y así evitar intromisiones de personal no autorizado.

Se instrumentaron varios sistemas de seguridad que garantizaban la integridad de la información en los diferentes puntos sensibles del programa. En primer lugar, en la comunicación entre los CEDAT y CENARREP; en segundo lugar, entre los CENARREP y los centros de difusión y, en tercer lugar, entre los centros de difusión e Internet.

"Entre las condiciones de seguridad que nos impusimos -comenta el Dr. Víctor Guerra- estuvo la de cuidar todos los aspectos que pudiéramos imaginarnos, más todos los que nos decían nuestros amigos y nuestros no tan amigos. Uno, por ejemplo, fue aislar eléctricamente a todo el PREP del resto del Instituto. El IFE esa noche iba a recibir a 2,000 personas, iba a haber 40 cadenas noticiosas conectando cámaras, reflectores, luces. Las posibilidades de cortos, de sobrecalen-

tamiento de las líneas, de los circuitos, de los transformadores, de los alimentadores, eran altísimas y entonces hicimos otro sistema eléctrico independiente del resto del Instituto, para que nuestra electricidad no estuviera sujeta a estos aspectos. Lo mismo se hizo con las líneas de fibra óptica para telefonía y para datos, se aislaron y se instalaron equipos contra incendio, contra inundación, contra humo, monitores para lo eléctrico y de seguridad, el aire acondicionado también estaba totalmente aislado. De tal manera que éramos autocontenidos en todo, como si estuviéramos en un bunker, no importaba lo que pasara afuera nosotros seguíamos teniendo nuestra comida, nuestra agua, nuestra electricidad, nuestro aire, etc. Efectivamente, el 6 de julio, por causas ajenas a nosotros y externas, hubo un corto circuito muy importante. Se fundieron la mitad de los circuitos. En otro lado se cayeron parte de las carpas y se mojó algo del equipo, pero una vez que se restableció la electricidad se disponía de un segundo equipo que pudo entrar a suplir. Todas las contingencias que pudimos haber imaginado estaban consideradas.

"El proyecto costó tres veces menos que en el 94. Para saber ahorrar hay que gastar bien, entonces donde había que comprar equipos pesados, se compraron equipos pesados, eso nos tendría que traer ahorros de otra manera; aislar eléctricamente nuestros centros de cómputo nos iba a traer ahorros en otros lugares. Al utilizar tecnología de redes o tecnologías bancarias probadas, si bien el costo de los equipos fue más de lo que se había pensado, la programación, la supervisión y el manejo costaron mucho menos."

Objetivos de seguridad:

Los objetivos que definieron la estrategia de seguridad fueron los mismos que rigieron la instrumentación global del Programa.
Confiabilidad – definida como la probabilidad de que el sistema cumpliera sus metas.
Seguridad – entendida como la capacidad de resistir ataques externos.
Credibilidad – concebida como la capacidad de convencer de que el Programa se ejecutaba correctamente.

Explica el Dr. Enrique Daltabuit: "La amenaza principal que tomamos en cuenta cuando estábamos hablando de cómo especificar el sistema de seguridad era la integridad de los datos, para que fuera

imposible (esto quiere decir en seguridad informática, algo muy especifico) alterar los datos, desde el momento en que entraran al sistema de información hasta que se difundieran a quienes debían verlos. La principal amenaza era la alteración de los datos en el tránsito y en el almacenamiento.

"La segunda amenaza, aunque menos importante, era la negación del servicio: que no se pudiera por alguna razón publicar esta información en forma oportuna.

"La primera la tratamos usando la criptografía, tecnología muy bien conocida, mediante las funciones de dispersión y la encripción con algoritmos estándar. Esencialmente usamos una variante de las firmas digitales.

"Para evitar la negación de servicio, esencialmente se pensó en que hubiera una multiplicidad de sitios donde se publicara la información y que se publicara en una forma reiterada, es decir, refrescada periódicamente para que si esa información era alterada, en la siguiente etapa de reconstrucción o refresco volviera a aparecer la información verdadera. La multiplicidad de sitios y de vías podría evitar la negación de servicio y las firmas digitales y refrescar la información con una cierta periodicidad evitaba la alteración de la información."

Principios:

Los principios bajo los cuales se diseñó la estrategia de seguridad para el PREP en 1997 se basaron en el objetivo fundamental que se intentaba alcanzar con el Programa y que era el de la absoluta transparencia del proceso electoral. Estos principios son los siguientes:

- *Participación* – se buscó involucrar a partidos políticos, medios informativos y organizaciones de observación electoral a fin de lograr un consenso en torno al diseño y ejecución del Programa, así como el convencimiento de que los resultados que se entregarían serían fidedignos.
- *Tecnología* – la seguridad no estaría basada en el secreto; se tenía presente que había demasiadas personas involucradas en la operación del Programa por lo que no sería tarea fácil conservar el secreto. Además, mantener ocultos aspectos cruciales del sistema obstaculizaría el buen desempeño e iría en contra del principio de transparencia. A este respecto, es importante mencionar que no

necesariamente las nuevas tecnologías de seguridad la garantizan de manera absoluta; en ocasiones hay métodos para invalidarlas que no fueron pensados por sus autores. Las tecnologías maduras que ya han sido probadas y que han resistido numerosos ataques sin fallar, podrían resultar más seguras.

- La tecnología de seguridad del PREP se basó, en gran medida, en sistemas de encriptamiento conocidos ampliamente, así como en técnicas de detección de alteraciones en documentos electrónicos y principios conocidos de teoría de la probabilidad.

Los sistemas a través de los cuales operó el PREP fueron diseñados utilizando tecnología de cifrado y autenticación. El objeto era que, a través de una serie de "paredes", "candados" y "pasaportes" informáticos, se impidiese completamente la alteración de la información electoral en tránsito a través de la red de comunicaciones, así como el acceso de manera no autorizada a los equipos de cómputo que intervenían en el proceso.

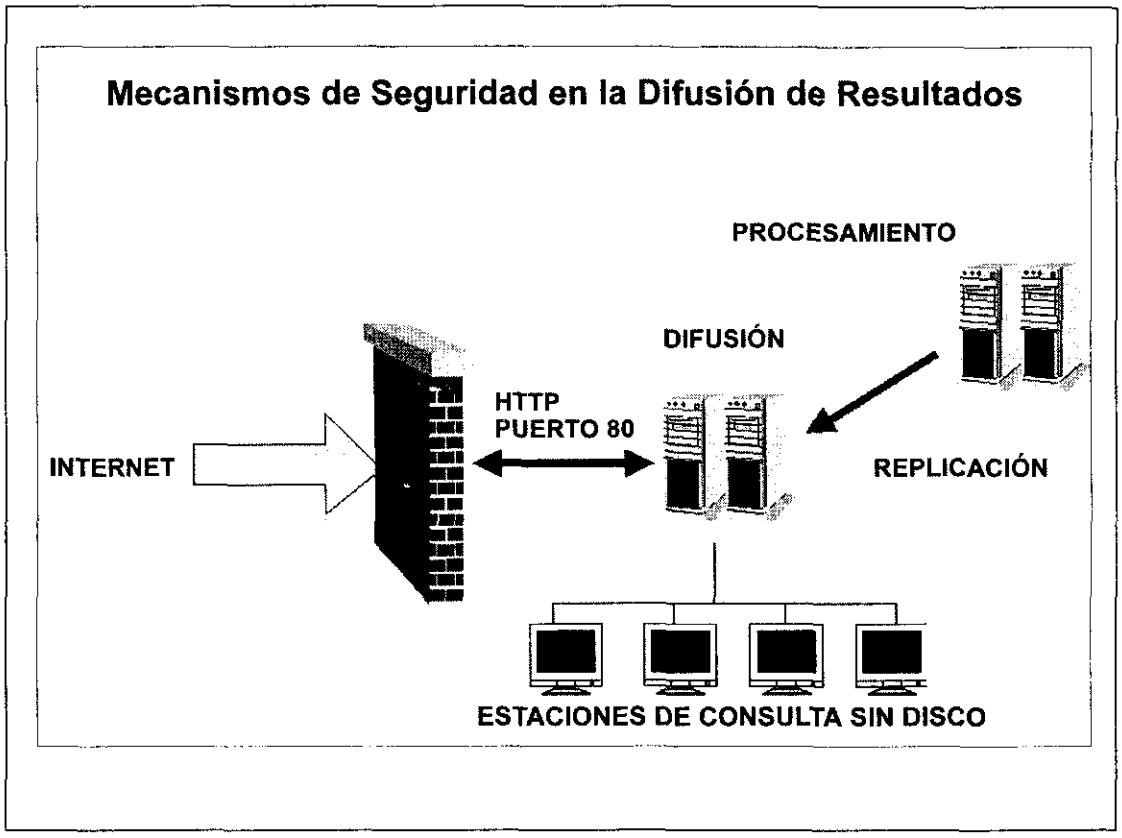
Cada transmisión de datos entre los CEDAT y el CENARREP, así como entre el CENARREP y el centro de difusión, era debidamente autentificada para verificar que realmente correspondiese a una transacción válida y autorizada. La información fue almacenada en una bitácora que registraba todos los eventos que estos centros de cómputo llevaban a cabo.

Por lo que respecta a la comunicación entre Internet y el centro de difusión, esta se protegió por medio de diversas "paredes" de seguridad que permitían que los usuarios de esta red internacional pudiesen observar los resultados electorales pero, bajo ninguna circunstancia, modificar esta información.

Intromisiones no autorizadas.

Uno de los aspectos más importantes de la seguridad del Programa consistía en la necesidad de evitar que hubiese programas desconocidos corriendo en alguna de las máquinas y que posibilitarían la entrada desde el exterior para modificar cifras electorales o para obstruir el funcionamiento de los sistemas.

Para prevenir una intromisión de esta naturaleza fue necesario evitar que se establecieran canales de comunicación encubiertos



funcionando entre los equipos de cómputo. Estos canales operan enviando información confidencial sin que quien vigile los canales de comunicación autorizados lo pueda detectar. Para establecer un canal encubierto es siempre necesaria la existencia de un programa especializado corriendo en cada una de las máquinas a comunicar.

Una posible solución a este problema consistía en seleccionar, de manera aleatoria, en la bodega misma del fabricante, la copia de los programas *UNIX* y *Oracle* a instalar en los equipos de cómputo. Para esto era necesario que el fabricante aceptase que el programa que se utilizara en el PREP fuese seleccionado directamente en su bodega inmediatamente antes de la elección y ante la vista de partidos, auditores u observadores. Sin embargo, esto presentaba un alto grado de dificultad y no se disponía del tiempo suficiente para hacerlo.

Autenticación de las transmisiones.

Para la autenticación de las transmisiones se utilizó una moderna tecnología de encriptado. Se crearon "pasaportes informáticos" lla-

mados firmas digitales criptográficas. Estas consisten en claves encriptadas para la identificación del origen de la información.

La criptografía es un método para hacer que un mensaje sea ininteligible para extraños a través de diversas transformaciones del texto original. En general, un método criptográfico es una función matemática reversible cuyo resultado depende del mensaje y de un parámetro o "llave". Si no se dispone de la llave, el tiempo necesario para interpretar el mensaje encriptado es tan grande, que para cuando un extraño lo logre, la información ya habrá perdido su valor.

El método de encriptado más conocido y aceptado es el DES o *Data Encryption Standard*, desarrollado hace más de dos décadas. La manera normal de usar el DES es un triple encriptado, es decir, el mensaje se encripta usando una primera llave; el resultado se vuelve a encriptar usando una segunda llave y, finalmente, este nuevo resultado se encripta usando una tercera llave. Cada una de las llaves usadas en DES es de 56 bits de longitud, lo que nos da una longitud total de 168 bits, más que suficiente para garantizar el nivel de seguridad requerido en el caso del PREP.

Para interpretar los mensajes encriptados con este método, se requiere probar todas las llaves posibles. Si la longitud de la llave es lo suficientemente grande, el tiempo necesario para probar todas las llaves es tan largo que, para cuando se tenga el resultado, la información no tendrá ningún valor.

En el caso del PREP se utilizó un algoritmo de encriptamiento con DES en modo triple y una llave para la terminal de captura remota, otra para el capturista y una última para el coordinador del CEDAT.

Los asesores de seguridad que tuvo el PREP, encabezados por el Dr. Enrique Daltabuit y el Ing. Guillermo Mallén, fueron quienes diseñaron el esquema general para el manejo seguro de datos. Como se mencionó antes, se partió de varios principios firmes, principalmente que la información contenida en las actas de escrutinio no es confidencial sino al contrario, pública y esto pudo corroborarse con el hecho de que, al término de la jornada electoral, en cada una de las casillas se publicaron inmediatamente los resultados para que los ciudadanos los conocieran. Por este simple hecho, la información a enviarse desde los CEDAT no podía estar encriptada pues esto iba en contra del principio de transparencia en la transmisión de los datos.

Sin embargo, si los datos de las actas no iban a transmitirse encriptados, se debía asegurar que nadie alterara la información desde que se capturara hasta que llegara al centro de cómputo y se difundieran los resultados de la misma. Por lo tanto, era necesario "firmar digitalmente" cada paquete de datos. De esta forma, se procedió a elegir el método de encripción para generar la firma digital que llevaría cada acta. Con el fin de tener la mayor transparencia posible en este proceso, se optó por basarse en algoritmos de encripción y autenticación que cumplieran con los estándares internacionales definidos para la seguridad en el manejo de la información. Así, para generar la firma digital se eligieron los algoritmos *MD5* para autenticación y *DES* para encripción, que son los más conocidos internacionalmente. Luego, se procedió a calcular el número de llaves que se requerirían para aplicar *DES* y a definir la forma como se aplicaría. El sistema *DES* funciona con llaves de 64 bits o el equivalente a 8 bytes. Para la firma digital de cada acta se optó por usar 3 llaves.

La utilización de los métodos *MD5* y *DES* triple en combinación para formar un "pasaporte" que acompañaría a los datos era un factor que se debía tomar en cuenta para dimensionar los equipos de cómputo puesto que si los datos estaban protegidos, el equipo que recibiera esta información debería ser lo suficientemente robusto para aplicar estos mismos métodos un número de veces por segundo y esto estaría determinado por el número de transacciones por segundo que se establecieran como límite para el proceso.

El equipo de comunicaciones que recibiera las llamadas de las terminales punto de venta debía ser un equipo integrado para evitar los inconvenientes de utilizar módems independientes, tarjetas descanalizadoras y de comunicación con el equipo de procesamiento central, además de que, considerando que debía soportar toda la carga y que cada CEDAT tendría al menos una línea telefónica privada para marcar al centro, el número de módem no podía ser menor a 360 por centro.

Por lo que respecta al equipo de cómputo que procesaría la información se consideró pertinente dividirlo por funciones: un equipo se dedicaría exclusivamente a mantener la base de datos y recibir la información del equipo de comunicaciones, en tanto que otro equipo recibiría la información del equipo que contenía la información y procesaría los datos para su presentación a los medios.

En 1994, las terminales permitían entrar a la aplicación con *passwords* o contraseñas. En ese entonces, se mandaron a los CEDAT los *passwords* para cada una de las terminales en papel. Sin embargo, esta solución presentaba el riesgo de que los *passwords* en papel se perdieran, además, los operadores de los CEDAT tenían que memorizarlos. Para el PREP97, se optó por no mandar las llaves en papel y aprovechar el recurso del lector de tarjeta que tienen incluido las terminales tipo punto de venta. De tal forma que la llave se almacenaría en una tarjeta de banda magnética que, al pasarla por la terminal, leería la llave para hacer la encripción de los datos.

En los CEDAT, quienes participaron en el proceso de captura de datos, fueron el coordinador, el supervisor y el capturista. El coordinador fue el encargado de inicializar las controladoras, esto por razones de seguridad y responsabilidad, mientras que el supervisor y el capturista se encargaron de abrir la sesión en una terminal de captura. Una TCR de captura no podía enviar datos si la controladora no había sido inicializada. Por lo tanto, se prepararon tres tipos de tarjeta magnética que almacenarían llaves distintas para el coordinador, el supervisor y el capturista.

El esquema de seguridad en la captura y envío de información no terminó ahí. Faltaba un detalle: la TCR de captura no tenía llave y no se podía enviar grabada en una tarjeta magnética. Se pensó entonces en la alternativa de que la controladora almacenara las llaves para las TCR y así se hizo. Cada controladora almacenó en su memoria *RAM* perdurable una secuencia de bytes suficientemente grande para generar las llaves que se requerían para las TCR de captura. Dicha secuencia midió 160 bytes (8×20), pensando en que de ésta se podrían generar hasta 20 llaves para 20 TCR; una cantidad suficientemente grande para un CEDAT, ya que el mayor se compuso de 12 TCR de captura y se pensó que era mejor que se dispusiera de capacidad redundante.

Se tenían entonces identificados cuatro tipos de llave: uno para los coordinadores, otro para los supervisores, uno más para los capturistas y uno para las TCR de captura. Sin embargo, había 3 tipos de tarjeta: la del coordinador, la del supervisor y la del capturista. Además, una política de seguridad que se adoptó fue que las llaves utilizadas en pruebas nacionales no fueran las mismas que se utilizarían en la jornada electoral. Sin embargo, se dejó la posibilidad

de utilizar una tarjeta de prueba nacional el día de las elecciones en caso de alguna contingencia.

El Ing. Guillermo Mallén, asesor de seguridad, comenta: "El objetivo básico del PREP era que los resultados de actas recibidos aparecieran y se difundieran exactamente iguales. La difusión se hacía básicamente por dos caminos, uno era el local, que tiene pocos problemas de seguridad y el otro era vía Internet, que tiene problemas graves de seguridad. Entonces, en última instancia, si la difusión por Internet tenía problemas de seguridad, cuando menos la difusión a la televisión, a la radio y a los medios en general no había tanto problema. El eslabón más débil de todos y el más problemático era asegurar que lo que se estaba metiendo en los CEDAT era lo mismo que se estaba recibiendo, esto era especialmente crítico porque TELMEX dijo que iba a amarrar las líneas telefónicas de los CEDAT para acá.

"Nuestro principal enfoque fue hacía la recepción, ¿cómo puedes estar seguro de que lo que te mandan está bien? Una manera es encriptarlo todo, lo cual, a su vez, tenía dos problemas: el tiempo de proceso de las terminales de los CEDAT que tenían un procesador con poca capacidad y, por otro lado, se supone que los votos son información pública y el encriptarlos iba en contra de la transparencia del proceso. El objetivo, entonces, era no encriptar. ¿Qué hicimos? Le pusimos una firma digital criptográfica que tiene la característica de que solamente la gente que tiene la llave puede generar esa firma, entonces, si mantenemos esas llaves bien cuidadas, sabemos que no nos van a falsificar los votos. Un bit que le cambien a esa información y la firma se hace totalmente diferente, entonces tenemos la manera de verificar que no ha sido alterada. Lo que nos interesaba era que no fuera a llegar información alterada y esto se resuelve con la firma. Cuando ustedes hablan de firma criptográfica, automáticamente todos los especialistas piensan en lo mismo, lo que se llama un sistema de llave pública y privada, ahora bien, aquí no usamos un sistema de llave pública y privada, porque computacionalmente este sistema de llave es verdaderamente muy pesado y si finalmente, después de muchos problemas, las terminales apenas pudieron trabajar con el DES, que es un sistema muy ligero, con el otro materialmente no hubiera sido posible.

"Luego están los centros de proceso, aquí la recomendación fue aislarlos, bueno había más o menos cierto nivel de aislamiento, no

perfecto. Había un punto relativamente débil en el enlace entre los dos centros, en donde cualquier empleado de TELMEX podía haber intentado intervenir las líneas. La ventaja que tuvimos es que la información que pasaba por ahí, pasaba con las firmas originales que venían desde los CEDAT y esa comunicación sí estaba encriptada. Ahí no había tanto problema", concluye el Ing. Mallén.

Normas de criptografía

El algoritmo de encripción que se utilizó fue el *Data Encryption Standard* (*DES*) en modo triple, con tres llaves diferentes para el supervisor, el capturista y la TCR. Debido a la forma en que funciona el algoritmo *DES* usado en las aplicaciones, los 56 bits se acomodaron en 8 bytes usando los 7 bits más significativos de cada byte. Desde el punto de vista práctico, lo más cómodo fue generar llaves de 64 bits aunque en realidad solamente se usaron 56. Se empleó la función de dispersión (*hash*) conocida como *Message Digest 5* (*MD5*) para establecer la huella digital de la información a transmitir. Una firma digital consistía de un *MD5* sobre el registro de datos encriptada con *DES* usando las 3 llaves mencionadas.

La firma digital se "pegó" al registro de datos, el cual se transmitió en claro.

El procedimiento que se siguió en la inicialización de las controladoras, en lo que se refiere a protección de la información, fue el siguiente:

1. Al encender la terminal controladora, esta pidió leer la tarjeta magnética del coordinador, de la cual obtuvo la llave y número de serie de la llave (número de tarjeta).
2. Se calculó una función de dispersión *MD5* del arreglo de números aleatorios (secuencia de 160 bytes). Para la identificación del CEDAT se envió al equipo de cómputo (CENARREP) el número de serie de la terminal controladora, el número de serie de la tarjeta del coordinador y el valor *MD5* encriptado usando *DES* simple con la llave del coordinador y codificado con *Radix64*.
3. El equipo de cómputo recuperó la llave del coordinador y el arreglo de números aleatorios y calculó nuevamente el valor de la función *MD5* enviada por la terminal, después envió de regreso un código de aceptación o rechazo encriptado con la llave de la terminal controladora.

4. La terminal controladora recibió el código de respuesta, lo desencriptó e indicó si hubo problemas. En caso de que hubiese algún error se repetía este proceso desde el principio. Si después de 3 intentos no había respuesta correcta, el coordinador CEDAT llamaba al PREP para solicitar instrucciones.
5. En el equipo de cómputo se registró en una bitácora todos los eventos que realizó cada CEDAT, incluyendo fecha y hora.
6. Una vez aceptada en el centro de cómputo, la controladora procedía a generar una llave para cada terminal de captura encriptando la secuencia de 160 bytes con la llave del coordinador.
7. La controladora enviaba a cada terminal de captura una llave de encripción y esperaba el código de respuesta. Los usuarios sólo pudieron usar las terminales cuyo código de respuesta fue correcto.

En cuanto a la seguridad en la información, se aplicó el siguiente proceso:

1. La TCR de captura leía las tarjetas de supervisor y capturista de las cuales obtenía ambas llaves con sus respectivos números de serie para habilitar una sesión.
2. La TCR de captura concatenaba su llave (que le fue proporcionada por la controladora) con las de capturista y supervisor. A esta concatenación le calculaba una función *MD5*, misma que encriptaba con la llave de la TCR y pasaba a formato *Radix64*.
3. La TCR enviaba a la controladora su número de serie, los números de serie de las tres llaves y el resultado calculado en el punto anterior.
4. La terminal controladora recibía la información de la TCR de captura y la enviaba al centro de cómputo.
5. El centro de cómputo recibía y verificaba la información de la TCR y enviaba un código de aceptación o rechazo encriptado con la llave del coordinador (llave de controladora) y registraba en su bitácora la transacción y el resultado de la misma.
6. La controladora recibía el código de respuesta y lo enviaba a la TCR de captura para que notificara al capturista si podía o no comenzar con la captura de actas. En caso de que el centro de cómputo rechazara a la TCR más de dos veces, se procedía a utilizar otra TCR de captura.
7. Cuando la capturista tenía que dejar la TCR de captura en forma temporal o definitiva o por cualquier causa, cerraba su sesión. La

TCR enviaba su identificación con el código de cierre de sesión encriptado con su llave, a la controladora.
8. La controladora enviaba la información del punto anterior al centro de cómputo.
9. El centro de cómputo desencriptaba el mensaje enviado por la controladora de cierre de sesión y, si era aceptado, procedía a marcar a esa TCR en su base de datos para no aceptar información de esa terminal hasta que se hubiese abierto la sesión nuevamente.
10. La controladora recibía y desencriptaba el código de aceptación y la enviaba a la TCR de captura.
11. Dependiendo del código de respuesta, la TCR bloqueaba o no la terminal. El capturista podía habilitar su sesión en cualquier momento.

El Ing. Guillermo Mallén comenta que "los Estados Unidos, dicen que por razones de seguridad nacional tienen prohibida la exportación de cualquier software o cualquier dispositivo físico que tenga criptografía lo suficientemente robusta para que no la pueda romper nadie. Sin embargo, cualquier método criptográfico, para que realmente sepamos que es seguro, tuvo que haber pasado la prueba del tiempo y la prueba del escrutinio de los criptógrafos de todo el mundo. La parte matemática se publica en las revistas de criptografía.

"Eso se hace para que todos los criptógrafos lo puedan examinar y el que encuentre por dónde atacarlo, estará perjudicando al otro. Entre ellos existe una gran rivalidad y eso es bueno para el negocio, por eso todos los algoritmos buenos de criptografía son públicos. Los otros países tomamos las matemáticas y lo volvemos a programar y nos queda algo que es igual de bueno que lo que está prohibido exportar y no estamos violando ninguna ley. Aunque ellos no permiten exportar, aquí no hay ninguna ley que diga que está prohibido importar un aparato de éstos y que además no hace falta, aquí los hemos desarrollado ya muchas veces y mucha gente sin la mayor dificultad."

Generación de llaves para controladoras y tarjetas magnéticas

Las controladoras almacenarían secuencias de bits suficientes para entregar llaves a las TCR de captura y esta encriptaría la información con 3 llaves distintas: la que le entregara la controladora, la del

supervisor y la de capturista. Por lo tanto, fue necesario generar llaves para controladoras y para 3 tipos de tarjetas diferentes: coordinador (tarjeta de controladora), tarjeta de supervisor y tarjeta de capturista. Para la generación de llaves se tomaron en cuenta los siguientes 2 puntos importantes:

En el proceso se emplearon números aleatorios producidos en un ambiente controlado mediante el ruido intrínseco producido por dispositivos electrónicos. Para este proyecto en particular se contó con la valiosa colaboración de la Universidad Anáhuac del Norte, la cual creó para el PREP 1997 un "Generador de Llaves". Este dispositivo consiste en un circuito que contiene un diodo *Zener*, una etapa de amplificación y un decodificador analógico/digital que digitaliza el ruido del diodo y los bits así obtenidos y los envía a una computadora a través del puerto paralelo. La computadora, a su vez, recibe los bits y los combina formando con ellos un archivo. Los bits generados se combinan mediante una operación *XOR* con una secuencia pseudoaleatoria con el fin de lograr una secuencia de bits en la que la probabilidad de que cada bit consecutivo sea un cero o un uno es la misma (50%).

Las personas que crearon el "Generador de Llaves" y que apoyaron al PREP en todo momento fueron el Ing. Jerry N. Reider, Coordinador de Telecomunicaciones y el Ing. Jorge Gutiérrez Vera, Director, ambos de la Escuela de Ingeniería de la Universidad Anáhuac del Norte

Con el fin de conservar la transparencia en el proceso electoral, para generar las llaves de encriptamiento se organizó un evento en la primera semana de junio en el Auditorio del IFE al cual se invitó a los representantes de partidos políticos. En este evento se hizo lo siguiente: para generar las llaves se utilizó una computadora *Acer Pentium* sin disco duro. Se arrancó desde un disco flexible con sistema operativo *DOS 6.22* y desde ahí se corrieron los programas que activaron el generador. Se generaron 2 archivos: uno de llaves para controladoras y otro para las tarjetas. El archivo de controladoras contenía 20,000 llaves o el equivalente a 160,000 bytes, mientras que el archivo de tarjetas contenía 12,000 llaves o el equivalente a 96,000 bytes.

El total de llaves que se requerían se obtuvo de la siguiente manera:

- Primero, para las controladoras se necesitaba un mínimo de 714 secuencias de 160 bytes, es decir, $714 \times 160 = 114{,}240$ bytes o el equivalente a 14,280 llaves. Por lo tanto, era necesario generar una cantidad mayor a ésta.
- Por otra parte, en el caso de las tarjetas se consideró que para coordinadores se requerían como mínimo 330 llaves para pruebas nacionales y otras 330 para la jornada electoral, para los supervisores se requería una cantidad igual, dado que había un coordinador y un supervisor por CEDAT: $330 \times 2 + 330 \times 2 = 1{,}320$ llaves requeridas para 2 tipos de tarjetas. Para las tarjetas de los capturistas se consideraron 3,000 llaves para pruebas nacionales y otras 3,000 para la jornada electoral. En total se requería un mínimo de $3{,}000 \times 2 + 1{,}320 = 7{,}320$ o el equivalente a 58,560 bytes. Obviamente, se debería generar una cantidad de llaves mayor a ésta.

Una vez generados los bits aleatorios con el "generador de llaves", la siguiente tarea fue hacer los programas que separaron las llaves y que generaron el formato que se requería para los programas de aplicación, tanto en los sistemas de cómputo como en los sistemas de captura.

Desde un principio se consideró utilizar llaves de 8 bytes (en *ASCII*), así que las empresas *Sun* y *Verifone* diseñaron sus programas tomando en cuenta este hecho. Sin embargo, al licitar las tarjetas de banda magnética se notó que sólo el *track* 1 almacenaba caracteres y estos eran alfanuméricos. Por lo tanto, las llaves no podían grabarse en código *ASCII* y fue necesario convertirlas a hexadecimal y, además, hacer uso del *track* 1. Esto se aplicó solamente a las llaves de las tarjetas; la secuencia de las controladoras no sufrió cambios. Todos los programas tanto de *Verifone* como de *Sun* consideraron 8 bytes para las llaves.

A mediados del mes de mayo las llaves definitivas no estaban aún listas y para las de programas de aplicación tanto de *Verifone* como de *Sun* se requería conocer el formato de las mismas, así que en el PREP se generaron algunas llaves de prueba. El proceso consistió en tomar un archivo ejecutable en *UNIX* y convertirlo a formato decimal con el comando uuencode/uudecode de *UNIX*. El propósito era obtener 30 llaves en forma manual del archivo resultante del comando anterior. Esta idea de convertir el código binario a decimal fue un error porque el comando de *UNIX* generaba caracteres no mayores a 7 bits y los

archivos ejecutables contenían caracteres de 8 bits. Así que la mitad de los caracteres *ASCII* no se estaban considerando.

Al generar las llaves de prueba, se grabaron algunas tarjetas de prueba también con las cuales se comenzaron a probar las aplicaciones de *Verifone*. Las tarjetas almacenaron solamente 2 datos: número de serie de la llave (6 caracteres) y la llave en código hexadecimal (16 caracteres).

Casualmente, de las llaves de prueba que se generaron desde *UNIX*, ninguna contenía caracteres mayores a 5F en hexadecimal, por lo que con estas tarjetas nunca hubo problema en las aplicaciones de las terminales. Es decir, las controladoras y TCR de captura, en las primeras pruebas de conexión con el Centro de Cómputo, siempre pudieron inicializarse y no se presentaron problemas de conectividad.

El primer programa que se diseñó para la separación de llaves, consistió en lo siguiente: los archivos de llaves (controladoras y tarjetas) contenían código binario puro, así que el programa solamente tenía que tomar, en el caso de las controladoras, secuencias de 160 bytes y ponerlas en otro archivo con un identificador consecutivo (número entero que sería el número de serie de esa secuencia). El mismo programa haría la misma operación pero con secuencias de 8 bytes.

Los primeros archivos que se generaron presentaron algunos inconvenientes, los tabuladores, saltos de línea y caracteres nulos ocasionaron desfasamientos en los archivos de llaves, los cuales no podían ser leídos directamente por los programas de aplicación puesto que ya se había definido ese formato y el problema era generar las llaves en el formato de prueba que se utilizó. Por lo tanto, fue necesario eliminar los caracteres problemáticos (tabuladores, saltos de línea y nulos), así que el programa, cuando leía alguno de estos caracteres, simplemente lo brincaba.

Una vez generadas las secuencias de controladoras (se obtuvieron aproximadamente 982 secuencias) se entregaron a *Sun* para que las subiera a sus tablas en *Oracle*. Por otro lado, para las llaves de las tarjetas no se siguió el mismo criterio de discriminación de caracteres y sí fueron incluidos los que no se consideraron para las secuencias de controladoras. Esto ocasionó algunos problemas.

Para las tarjetas se deberían generar las mismas llaves pero con formato en hexadecimal como ya se había mencionado, por la banda

de codificación. A *Sun* se le entregaron en *ASCII* y el archivo con formato en hexadecimal se usó para la grabación de las tarjetas; aparentemente no había problemas. Sin embargo, a la par se había ya realizado la carga de terminales (se invirtió una semana en esta tarea y una gran cantidad de gente) y se había comenzado con el grabado e impresión de las tarjetas (aproximadamente se llevaban 1,000), se comenzó a probar las primeras tarjetas grabadas con las primeras terminales cargadas y la sorpresa fue que ninguna controladora se podía inicializar, así como ninguna TCR de captura. Se procedió entonces a investigar la razón de este problema y se llegó a la conclusión de que la causa estaba en las terminales, resultó que el lector de tarjeta incorporado a las terminales era de 7 bits y leía solamente caracteres no mayores a 7F, dado que en las tarjetas de crédito solamente se graba el nombre y algunos caracteres numéricos, pero ninguno mayor a 7F. El problema logístico era grave porque las terminales estaban listas para repartirse en los CEDAT. Existían 2 alternativas a seguir: una era modificar la aplicación para que por software el lector pudiera leer 8 bits, pero se requería recargar las terminales lo cual implicaba perder una semana de trabajo y la otra, grabar nuevamente las tarjetas magnéticas con los nuevos códigos. Finalmente, la decisión fue que en las llaves se apagaran los 2 bits más significativos, quedando entonces de 8 bits con los 2 primeros siempre cero. De esta forma, lo más que se podía representar era el carácter 3F. En resumen, *Verifone* no había considerado en sus aplicaciones leer 8 bits completos del lector.

Una vez que se volvió a grabar las tarjetas magnéticas y al seguir probando con las terminales, resultó que algunas se podían inicializar y otras no. Al investigar el problema se llegó a la conclusión de que la causa estaba nuevamente en las terminales. Ahora, las tarjetas tenían caracteres nulos y el lenguaje C trunca una cadena cuando se encuentra un nulo. Por lo tanto, las aplicaciones de *Verifone*, al leer una cadena con carácter nulo, truncaban la llave y el *DES* no coincidía con el del centro de cómputo. Esta era la razón por la que las terminales no se podían inicializar. Era necesario entonces separar, de entre 3,900 tarjetas de capturista que se debían utilizar en las pruebas nacionales, aquellas que contenían un carácter nulo. Se modificó por segunda vez el programa para generar las llaves de las tarjetas y se grabaron nuevamente. La modificación que se hizo al

programa fue cambiar el carácter nulo por "@" que tiene código hexadecimal 40 y así fue como quedaron finalmente las llaves.

De las 3,900 tarjetas que ya se habían entregado, 150 que tenían caracteres nulos no se recuperaron puesto que ya estaban en las cajas enviadas a los CEDAT. Así que se sabía que algunas tarjetas fallarían en las pruebas nacionales. Afortunadamente las de la jornada electoral no presentaban este problema.

Por último, días antes de las elecciones se optó por generar nuevamente las tarjetas de coordinador. El argumento fue que las llaves para la jornada electoral ya se habían expuesto en las tablas en *Oracle* y ya no eran tan seguras. Se procedió a la realización de otro programa; como ya no se podían generar nuevas llaves, se optó por hacer uso de los archivos de llaves de controladoras y tarjetas. Se pensó en hacer una *OR* exclusiva byte a byte entre los archivos de llaves y luego pasar el resultado por una *AND* con 3F. De esta forma, se generaron nuevas llaves utilizando los archivos originales.

En resumen, en esta actividad existieron 3 programas: el que generó las secuencias de controladora de 160 bytes (en total se generaron 982 secuencias base), el que generó las llaves para las tarjetas en código *ASCII* (este programa fue el que apagó los bits más significativos de las llaves y cambió el carácter nulo por una "@", el archivo resultante fue el que se entregó a *Sun* para subir a *Oracle*) y el que convirtió a código hexadecimal las llaves del programa número 2 (el archivo resultante fue el que se empleó para la grabación de las tarjetas magnéticas). Este programa generó las nuevas llaves para las últimas 2,000 tarjetas haciendo uso de los archivos de llaves de controladoras y de tarjetas.

Es importante mencionar que en ninguno de los 4 casos anteriores se obtuvieron llaves repetidas. Todo resultado de los programas se validó con el comando *uniq* y *sort* de *UNIX* con el fin de asegurar que todas las llaves fueran únicas, tanto para controladoras como para tarjetas.

La segunda semana del mes de junio fue programada para la carga de terminales tanto de captura como controladoras. La realización de esta tarea estuvo a cargo de *Verifone*. El personal de la Dirección de Transmisión de la Información y Evaluación Técnica del PREP participó también en estas actividades, supervisando la carga, auditando las terminales y generando los discos de carga y auditoría. Estos

discos contenían exclusivamente los archivos ejecutables y el sistema operativo para arrancar desde disco flexible, por lo que las computadoras que se utilizaron para la carga no tenían disco duro.

Después de esta carga, durante las pruebas nacionales se regresó el equipo que se había desconfigurado y fue necesario recargarlo y sustituirlo por uno nuevo. Esta actividad duró desde el 15 de junio hasta el día de las elecciones.

Al cargar la aplicación en las terminales controladoras también fue necesario llevar a cabo la carga de llaves, así como la carga de números telefónicos. A cada controladora se le cargó una secuencia base, un *offset* de 6 bytes y una cadena de 160 bytes de la cual, a partir de ella, la controladora generaría las llaves necesarias para las TCR de captura.

Se generó un disco de carga de llaves el cual contenía sistema operativo DOS 6.22 y los archivos necesarios para cargar las llaves en las controladoras, la computadora que se utilizó para esta carga no contenía disco duro.

El contrato de adquisición de las tarjetas magnéticas se asignó a la empresa Técnica Comercial VILSA, S.A. de C.V. y el PREP comenzó a trabajar con ella inmediatamente. En las bases del anexo técnico de la licitación (Invitación Restringida) mediante la cual se efectuó la adquisición, se especificó que el participante ganador proporcionaría el equipo necesario para la grabación de las tarjetas, así como el soporte técnico necesario y que dicha grabación se llevaría a cabo en las instalaciones y por el personal del PREP. De esta forma, VILSA entregó al PREP las tarjetas nuevas en blanco, así como un equipo para realizar el grabado e impresión de las mismas y se limitaron a asesorar técnicamente al personal del PREP en el manejo del grabador. El PREP grabó 12,000 tarjetas en total, en una primera fase se grabaron 10,000 y días después las restantes 2,000.

Como se especificó en la tarea correspondiente a la generación de llaves, ya se había comenzado con el grabado de las tarjetas cuando se tuvo que parar la actividad y volver a generar las llaves que se grabarían en la banda de codificación. Se habían grabado 1,000 tarjetas cuando se percató del cambio, así que se volvieron a grabar. Luego, cuando se notó el problema con el carácter nulo, se habían grabado cerca de 5,000 tarjetas y al volver a generar las llaves, se tuvieron que grabar todas las tarjetas que contenían caracteres nulos.

Por otro lado, para capturistas se envió a cada CEDAT la cantidad equivalente a las TCR de captura y 3 tarjetas de reserva. Todas las tarjetas eran diferentes entre sí hasta en número de folio. Para los coordinadores y supervisores, se enviaron tarjetas de respaldo, es decir, cada uno recibió dos tarjetas idénticas que contenían el mismo *offset*, la misma llave y el mismo número de folio.

Como ya se mencionó, se requerían al menos 7,320 llaves y la misma cantidad de tarjetas; se generaron entonces 12,000 llaves para las tarjetas y las tarjetas de supervisor y coordinador se hicieron por duplicado. De este modo, la cantidad de 7,320 aumentó a $7{,}320 + 660 \times 2 = 8{,}640$ tarjetas. Se generaron 9,600 tarjetas incluyendo algunas de reserva para capturistas, supervisores y coordinadores.

Seguridad de los centros de cómputo

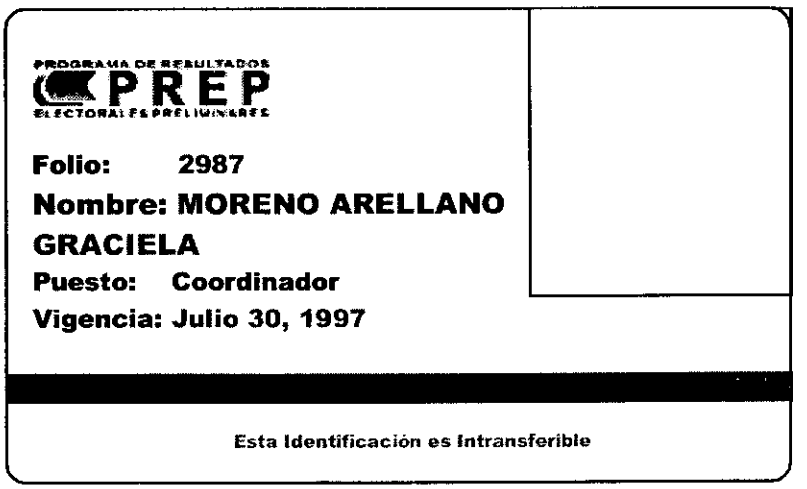
Dadas las condiciones de seguridad que el programa requería, hubo necesidad de instalar un sistema que asegurara físicamente al centro contra cualquier intromisión o accidente, para lo cual se convocó a una licitación cuyas bases definían los siguientes requerimientos:

- Centro de mando.
- Sistema de Control de acceso.
- Circuito cerrado de Televisión (CCTV).
- Central de alarmas.
- Sistema de detección de incendios

Se llevó a cabo el diseño, valuación, búsqueda de proveedores prospectos y finalmente la coordinación de la integración del sistema automatizado de seguridad física de las distintas áreas que comprendía el PREP.

Dicho proyecto fue asignado de forma directa a la empresa Matra Communications de México, S.A. bajo la representación del Ing. Jorge Rodríguez Leitao. Este sistema comprendía un control de acceso, central de alarmas y circuito cerrado de televisión. Su funcionamiento es simple: a cada empleado de las distintas áreas se le asignó una tarjeta de lectura magnética de proximidad y un código numérico, ya que los distintos accesos requerían de ambas para poder ser abiertos. Este sistema de seguridad se basaba en acceso discriminado a zonas definidas para los distintos tipos de personal, el cual se clasificó de acuerdo a sus actividades.

Ejemplo de tarjeta de lectura magnética utilizada en el PREP:



Con el circuito cerrado de televisión se cubrieron totalmente las áreas de cómputo, los pasillos interiores y los exteriores del área del sótano del edificio C, así como de su planta baja. Dentro del área del sótano se determinó ubicar el cuarto de control del sistema, contando para ello con un equipo de cómputo capaz de controlar la central de alarmas y el control de acceso, así como los monitores del circuito cerrado. El objetivo del circuito cerrado de televisión era garantizar que toda persona que ingresara al centro fuera registrada en video y poder proceder, en caso de algún imprevisto, a su identificación.

Por otro lado, las oficinas que albergaron el centro de cómputo alterno del PREP en el World Trade Center fueron custodiadas, desde la llegada de los equipos, por elementos de la policía auxiliar asignados por el propio cuerpo de seguridad del IFE, cumpliendo turnos de 24 horas con dos elementos a la vez. Estos reportaban a su agrupamiento y al jefe de este departamento y tenían instrucciones de permanecer dentro de las oficinas y no en áreas generales de la torre. Se encontraban equipados con armas medianas y chalecos antibalas, siendo su función la de salvaguardar todo lo existente dentro de las oficinas, así como al personal que laboró dentro de ellas.

Para la operación de los centros de cómputo se establecieron las siguientes normas generales:

- El acceso a la consola estaba restringido al personal autorizado.
- Las cuentas de usuario sólo se daban de alta cuando eran indispensables para la realización del proyecto el uso de las mismas.

- La cuenta general de administración (*root*) tenía las siguientes características:
  - sólo se utilizaba cuando era estrictamente necesario,
  - sólo un número restringido de personas estaba autorizado al conocimiento de la contraseña de superusuario,
  - se debía tener una cuenta de administración para realizar las actividades de rutina y gestión de recursos; esta cuenta debía otorgar solo los privilegios indispensables para que cada quien realizara sus tareas.
- Las actividades realizadas mediante estas dos cuentas debían ser respaldadas en discos, los cuales eran guardados bajo llave.
- Sólo dos responsables estaban autorizados al conocimiento de la contraseña del administrador general; además dicha contraseña debía ser resguardada en una caja fuerte.
- Cualquier tipo de cambio en la configuración del equipo tenía que ser autorizada y justificada; así mismo debía ser específicamente documentada.
- Todas las cuentas de usuario en el sistema estaban restringidas al uso para el cual fueron creadas.
- Todos los usuarios debían ser monitoreados para conocer el uso de sus cuentas. Este monitoreo se llevaba a cabo de la siguiente manera:
  - se tenían que revisar todas las bitácoras del sistema en un período máximo de 1 día,
  - se tenían que generar bitácoras ocultas, mediante programas que permitieran conocer las actividades que realizaban el sistema y los usuarios,
  - la información sobre la ubicación y el acceso físico del software y manuales del equipo, así como la documentación de los sistemas y sus fuentes, estaba restringida, por lo que solo el personal autorizado podía utilizarlo.

También se establecieron reglas específicas:

- Asegurar que no se instalase ningún otro software que representase un riesgo para la integridad de la información. Los usuarios tenían prohibido cualquier tipo de instalación de software y aplicaciones, sin importar el tipo que fuera; ya que podían ser un peligro latente para seguridad e integridad del sistema.

- Se revisaban los mecanismos de autenticación entre los centros de procesamiento, tanto a nivel de equipo como a nivel de información.
- Se supervisaba la capacitación al personal para el manejo de usuarios en el sistema de control de acceso, para poder dar de alta, baja o modificar usuarios en el mismo. Todos los usuarios tenían prohibido el uso de cualquier conexión fuera de la red local.
- Todos los usuarios debían mantenerse monitoreados para conocer el uso de sus cuentas. Este monitoreo se llevaba a cabo de la siguiente manera:
  - se debían revisar todas las bitácoras del sistema en un periodo máximo de 1 día,
  - se debían generar bitácoras electrónicas, mediante programas, las cuales permitían conocer las actividades que realizaban el sistema y los usuarios.
- Los respaldos eran completos, realizados en los equipos HA y PDB con el comando ufsdump. Además era necesario exportar la base de datos del PDB. Estos respaldos eran efectuados diariamente y en caso de no poderse hacer por que se estuviese utilizando el equipo, ya que no se podía dar de baja, se hacía un *tar* de las particiones principales.

Seguridad en la transmisión a Internet

Para la difusión de los datos se introdujo un factor que no había estado presente en ningún proceso electoral pasado: la difusión por Internet. El hecho de introducir a Internet como medio de difusión trajo como principal consecuencia la necesidad de proteger contra ataques a los equipos, reforzando los esquemas de seguridad que hasta el momento se habían previsto. Se utilizaron *firewall* modelo *Firewall-1* entre las líneas que comunicaban ambos centros y en la salida a Internet.

Opina el Dr. Enrique Daltabuit sobre la seguridad el día de la jornada electoral: "Desde el punto de vista de integridad de los datos no hicimos los cálculos de la capacidad de algún enemigo potencial, porque evidentemente el grado de seguridad depende de quién sea el enemigo. Es decir, un enemigo infinitamente inteligente e infinitamente rico puede romper casi cualquier sistema de seguridad. Un estudiante de secundaria con una máquina 286 no hace absoluta-

mente nada. El enemigo es el que define qué tan seguro es el sistema. Tomando los conocimientos convencionales, los algoritmos que se usaron no podían ser descifrados, es decir, no se podían romper las llaves en el tiempo que duró el proceso del PREP. Ninguna computadora ni ninguna combinación de computadoras que pudiéramos imaginar hubiera logrado romper una llave en las 8,10 ó 12 horas que duró el proceso. Hay que tomar en cuenta, además, que cada terminal de captura tenía una llave diferente. Pensar que alguien pudiera romper el número suficiente de llaves para afectar el resultado de la elección en el tiempo que duró el PREP para mí es totalmente imposible. El alterar los resultados en alguna de las páginas publicadas sería facilísimo, pero si estamos refrescando cada 5 ó 10 minutos, cualquiera que las quiera modificar tiene que tomarlas y manejarlas. Yo creo que tampoco hubiera sido factible el ataque de negación de servicio.

"Por seguridad se entiende que la información que se desea publicar se publique en los tiempos y modos que uno lo quiere hacer. En otros países, en otros sistemas, no se requiere de una centralización de la información antes de que sea publicada, sino que cada sitio de recolección de información la publica directamente en cuanto se captura. Entonces cada quien -los agentes de prensa, los partidos políticos, los analistas- tienen el trabajo ellos mismos de recoger la información. El problema se presenta cuando se ponen todos los huevos en una misma canasta. Pero dada la legislación que tenemos yo creo que el equipo del PREP hizo un trabajo excelente en la seguridad de informática", concluye el Dr. Daltabuit.