VII. Seguridad

La seguridad en el PREP 2000 fue importante debido a que su función primordial era brindar total protección al sistema contra cualquier boicot o posibles agresiones, así como prevenir cualquier tipo de contingencia que pudiera ocurrir. Debían de considerarse muchos aspectos ya que existía un temor generalizado por la posibilidad de atentados.

Se determinó un esquema de seguridad en el cual se evitó que sucediera cualquier incidente informático, se aseguró que la información contenida en las actas recibidas en los CEDAT coincidiera exactamente con la publicada, y que si alguien pretendiera descalificar el proceso electoral encontrara en el PREP 2000 un obstáculo para ello. Para esto se contó con la experiencia del Dr. Enrique Daltabuit y del Ing. Guillermo Mallén, quienes participaron en el Programa de 1997 y nuevamente fueron los asesores de seguridad para este PREP 2000.

Los elementos que definieron la estrategia en la protección del PREP fueron:

1. *Seguridad*. Resistir ataques externos.
2. *Confiabilidad*. Capacidad para que el sistema cumpliera sus metas.
3. *Credibilidad*. Convencer de que el Programa se ejecutaba correctamente.
4. *Transparencia*. Claridad de todos los métodos y procedimientos.

En el diseño de la estrategia de seguridad también se consideraron dos aspectos importantes:

- *Participación*. 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 habían demasiadas personas involucradas en la operación del Programa

> y mantener ocultos aspectos cruciales del sistema obstaculizaría el buen desempeño e iría en contra del principio de transparencia. En la actualidad, no necesariamente las nuevas tecnologías garantizan la seguridad de manera absoluta, existen algunas que ya han sido probadas y que han resistido numerosos ataques sin fallar que podrían resultar más seguras. Es por esto que la tecnología de protección del PREP 2000 se sustentó, en gran medida, en los sistemas de encriptamiento conocidos ampliamente, así como en técnicas de detección de alteraciones en documentos electrónicos y principios conocidos de teoría de probabilidad.

Con el fin de tener la mayor transparencia posible en este proceso electoral, los sistemas a través de los cuales operó el PREP 2000 fueron diseñados utilizando tecnología de cifrado y autenticación. Así, para generar la firma digital de cada acta se optó por basarse en algoritmos MD5 para *autenticación* y DES para *encripción*, que son los más conocidos internacionalmente para la seguridad en el manejo de la información.

La *autenticación* es el proceso de verificar la identidad de usuarios o procesos de cómputo. El cifrado es el resultado de la criptografía que involucra operaciones matemáticas para proteger la información.

La integridad de los datos debía protegerse desde el momento en que entraran al sistema hasta que se difundieran. La amenaza principal era la alteración de los datos en el tránsito y almacenamiento; para cubrir este punto se usó la criptografía, tecnología muy bien conocida, es decir, la encripción de los datos con algoritmos estándar y usando firmas digitales.

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 (texto) y de un parámetro o "llave". Si no se dispone de la llave, el tiempo necesario para interpretar el mensaje es tan grande que para cuando un externo lo logre, la información ya habrá perdido su valor.

El método de encriptado más conocido y aceptado es el DES *(Data Encryption Standar)*, desarrollado hace más de dos décadas. La manera en la que se usó el DES fue un triple encriptado, es decir, el mensaje se encriptaba usando tres llaves. Cada una de las llaves usadas en el DES eran de 56 *bits* de longitud, lo que generaba una longitud total de 168 *bits*, un nivel más que suficiente para garantizar la seguridad requerida.

Para interpretar los mensajes encriptados con este método se requería probar todas las llaves posibles. Si la longitud de las llaves era lo suficientemente grande, el tiempo necesario para probarlas todas sería aún mayor, por lo tanto, para cuando se lograran descifrar ya habría pasado un lapso considerable.

El objeto era que, a través de una serie de "paredes", "candados" y "pasaportes" informáticos se impidiese 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.

Generación de llaves para procesos criptográficos

Para aplicar el encriptamiento y la generación de firmas electrónicas se debía producir un número de llaves suficientes; se hizo el cálculo de las que se requerían para el DES, el cual funciona con llaves de ocho *bytes*. Cada una de las llaves utilizadas era de 56 *bits*, pero debido a la forma en que funciona su algoritmo utilizado en las aplicaciones se requería que las llaves fueran de una longitud de 64 *bits*, es por esta razón que los 56 *bits* se acomodaron en ocho *bytes* usando los siete *bits* más significativos de cada *byte*.

Las características estadísticas de las llaves fueron las siguientes:

a) Su aleatoriedad debía ser uniforme, es decir, que todos los rangos de llaves tuvieran la misma probabilidad de ocurrir.

b) Que no existiera correlación serial entre las llaves, en el sentido de que dada una cadena de llaves sucesivas, la siguiente llave en la serie tiene la misma probabilidad de ocurrir, independientemente de cuál sea la cadena que le precede y aunque se tuviera un historial de llaves antecesoras, una predicción es esencialmente equivalente a adivinar la siguiente llave, es decir, que el conocimiento de las antecesoras no mejora la predicción.

c) Deberían ser llaves únicas, no debía repetirse ni una sola, por lo que se manejaron probabilidades muy reducidas para garantizarlo.

d) Las claves generadas debían ser de forma tal que no pudieran ser descifradas por persona alguna, independientemente de su experiencia y conocimiento en el área de la informática, ni por equipo alguno, ejecutando algún programa sofisticado tendente a la ruptura de estas claves, por lo menos no en el momento en el que la información tuviera valor, ya que sabemos que se pueden romper claves pero se requeriría de cierto tiempo para hacerlo.

Al respecto, se suelen emplear programas de computadora orientados a la generación de códigos *pseudoaleatorios* para desarrollar estas claves, pero el resultado no es del todo perfecto porque eso implica cierto nivel de *predictibilidad* y la llave resultante puede ser violada si se dispone de ciertos parámetros.

En el proceso de generación de llaves se emplearon caracteres aleatorios en un ambiente controlado mediante el ruido intrínseco producido por dispositivos electrónicos.

El "generador de llaves", creado desde el PREP 1997, es un dispositivo consistente en un circuito que contiene un diodo *Zener*, una etapa de amplificación y un decodificador que digitaliza el ruido del diodo obteniéndose los *bits*, los cuales se envían a una computadora a través de uno de sus puertos de comunicaciones llamado puerto paralelo, la computadora los recibe y los combina formando con ellos un archivo. Los *bits* generados se combinan mediante una operación a nivel de *bits* o *booleana* (XOR), con una secuencia *pseudoaleatoria*. El fin es lograr una secuencia de *bits* con la misma probabilidad de que cada *bit* consecutivo sea un cero o un uno (50%).

Este dispositivo se basa en el fenómeno físico relativo al ruido eléctrico natural existente en todos los dispositivos electrónicos, las secuencias resultantes son de naturaleza más puramente aleatorias y, por consiguiente, más difíciles de predecir en comparación con aquellas desarrolladas mediante programas especiales para computadora.

Una medida de seguridad fue que las llaves utilizadas en las pruebas nacionales no fueron las mismas que se usaron el día de la jornada electoral, con lo que se garantizó que nadie las conociera y permanecieran bien resguardadas.

Requerimientos de llaves

- Se necesitaba un mínimo de llaves para las terminales de captura remota que se almacenarían en las terminales controladoras. Se decidió generar 16,000 agrupadas en secuencias de 20, lo que daba un total de 800 secuencias. Esto es: 800x160=16,000 llaves de ocho *bytes*=128,000 *bytes*.
- Para las tarjetas se consideraron 300 llaves de coordinador, 300 de supervisor y 3,388 para capturista, multiplicado por dos debido a que se generaron llaves para pruebas nacionales y para el día de la jornada electoral. Esto es: (300x2)+(300x2)+(3388x2)= 7,976 llaves de ocho *bytes* = 63,808 *bytes*.
- El total de llaves que se generaron fue 24,000.

Seguridad en la captura

El proceso de captura podía ser susceptible a que alguna persona o grupos tuvieran interés en modificar la información electoral o introducir votos no legítimos al sistema, por lo que se necesitaba reconocer e identificar a cada uno de los puntos desde los cuales se capturaría, lo que se solucionó con un proceso de autenticación muy riguroso basado en la implementación de las llaves para garantizar que el alta, baja, captura y transmisión desde algún equipo de cómputo fuera una operación válida y reconocida por el sistema. A pesar de que se diera el caso de que alguien contara con el mismo equipo de cómputo, con la tecnología y las herramientas del programa no podría engañar al sistema, ya que las terminales permitían entrar en la aplicación sólo por medio de contraseñas.

Participaron en el proceso de captura de datos: el coordinador, el supervisor y el capturista. Los dos primeros fueron los encargados de inicializar las controladoras (por razones de seguridad y responsabilidad), el supervisor y el capturista se encargaron de abrir la sesión en una terminal de captura. Una TCR no podía enviar los datos si la controladora no había sido inicializada. Por lo tanto, se generaron tres tipos de tarjeta magnética que almacenaría llaves distintas: una para el coordinador, otra para el supervisor y una para cada capturista, de acuerdo al número de TCR en cada CEDAT.

Se generaron dos juegos de tarjetas, uno para usarse durante las pruebas nacionales y otro para usarse durante la jornada electoral.

Debido a que la TCR no tenía llave y no podía ser grabada en una tarjeta magnética, la controladora almacenó sus llaves. Cada controladora guardó en un dispositivo conocido como memoria de acceso aleatorio perdurable (*Random Access Memory*) una secuencia de *bytes* suficientemente grande para generar las llaves que se requerían para las TCR de captura. Esta secuencia midió 160 *bytes* (8x20), de la cual se podían generar hasta 20 llaves para TCR.

La carga de llaves para las terminales punto de venta se realizaría únicamente en las controladoras. Sin embargo, el centro de cómputo guardaría una relación de las que correspondían a cada tipo de usuario, así como el número de serie de cada una de las llaves, y en el caso de las tarjetas magnéticas identificaría también si la llave correspondía a una prueba nacional o a el día de las elecciones.

Al encender la terminal controladora ésta pedía leer la tarjeta magnética del supervisor y del coordinador, de la cual obtenía llave y número de serie (número de tarjeta). Se preparaba un paquete de información llamado criptograma que pedía la autorización

al CENARREP identificando el equipo que quería comenzar a operar. Si el CENARREP lo conocía y podía descifrar el criptograma con las claves acerca de ese equipo le respondía y permitía el acceso. Una vez aceptado en el centro de cómputo, la controladora procedía a generar una llave para cada terminal de captura, la enviaba y esperaba el código de respuesta.

Todo este esquema de llaves se utilizaría para la autenticación y también para proteger la información que debería viajar sin encripción, pero con normas de seguridad que garantizaran su consistencia y confiabilidad.

Una vez que todo estaba listo para realizar la captura, se debía garantizar que no existieran errores en ésta, que la información contenida en cada acta fuera exactamente la misma que se introdujera al sistema, por lo que el sistema interno de cada terminal de captura remota pedía que se registraran dos veces los datos para su validación, si éstos coincidían la operación procedía, de lo contrario se repetía el procedimiento hasta que no existieran errores.

Seguridad en la transmisión

Un punto sensible en la seguridad fueron las líneas telefónicas de comunicación que se usaban para recibir los datos de captura, que aunque eran privadas corrían el riesgo de ser intervenidas, sin embargo, no tenía sentido proteger la captura aplicando métodos de autenticación para cada equipo que se quisiera capturar, si cuando esta información se transmitiera podría ser vulnerable a cualquier ataque.

Se cuidaron esencialmente las comunicaciones y se trabajó en conjunto con la empresa encargada de dar este servicio para procurar líneas libres de ruido y seguras desde los CEDAT hasta el CENARREP.

La información contenida en las actas de escrutinio no era confidencial, sino al contrario, fue pública. Al término de la jornada electoral, en cada una de las casillas se publicaron inmediatamente los resultados para que los ciudadanos los conocieran; 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.

Si los datos de las actas no iban a transmitirse encriptados, se debía asegurar que nadie alterara la información desde su captura hasta que llegara al centro de cómputo y se difundieran los resultados de la misma, por lo que era necesario firmar digitalmente cada paquete de datos. Se eligió el método de encripción para la firma digital que llevaría cada acta.

Mediante la firma digital criptográfica se aseguraba que solamente la persona que tuviera la llave podía generar esa firma. Si se mantenían esas llaves bien cuidadas, se sabía que no se alteraría la información de captura. Con tan sólo un *bit* que fuera alterado haría la firma totalmente diferente.

Además de establecer que un mensaje no había sido alterado, se debía verificar que cada transmisión provenía de su emisor. La información fue almacenada en una bitácora que registraba los eventos que los centros de cómputo llevaban a cabo.

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 modems independientes, tarjetas descanalizadoras y de comunicación con el equipo de procesamiento central, además, 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 modem no podía ser menor a 360 por centro.

Seguridad en el procesamiento

En la contabilización de los votos se tomaron en cuenta varios aspectos de seguridad: no considerar datos erróneos, ya fuera porque el capturista se hubiera equivocado en el acta o alguien hubiera intentado ingresar en el sistema con información falsa; con la aplicación de diversos algoritmos de programación se verificaba el número de votantes, con lo cual no se podían ingresar más votos de los especificados por cada distrito en la base de datos; el algoritmo implementaba una serie de validaciones y según la gravedad de la inconsistencia, no contabilizaba las actas que no coincidieran con la base de datos. Estas actas serían revisadas después en el conteo oficial por todos los partidos políticos. Así fue como se decidió validar el conteo de la elección.

Se definieron varias políticas de seguridad, normas generales y aspectos de contingencias:

- *Seguridad física*. Control de acceso en instalaciones clave, como fueron los CENARREP y CEDAT, tanto para visitantes como empleados, alta y baja de los equipos de cómputo, mantenimiento, manejo de medios de almacenamiento electrónicos y respaldos, sistemas de aire acondicionado, protección contra incendios, terremotos, inundaciones.

- *Seguridad en la información*. Se tomaron medidas para la prevención de virus, identificación, control de la información impresa, integridad, confidencialidad y licencias de *software*. En las cuentas, su tipo, asignación y contraseñas.
- *Seguridad de la red*. Se consideraron los accesos remotos, *firewalls*, WWW, correo electrónico, FTP.

Seguridad en los centros de cómputo

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

- El acceso a cualquier computadora estaba restringido, sólo se permitía al personal autorizado.
- Las cuentas de usuario sólo se daban de alta cuando eran indispensables para la realización del proyecto.
- La cuenta general de administración (*root*) tenía las siguientes características:
  - Sólo se utilizaba cuando era estrictamente necesaria.
  - Sólo un número restringido de personas tenía autorización de conocer la contraseña de superusuario.
  - Se debía tener una cuenta de administración para realizar las actividades de rutina y gestión de recursos.
- Las actividades realizadas mediante las cuentas debían ser respaldadas en discos, los cuales eran guardados.
- Sólo los consultores en seguridad responsables tenían conocimiento de la contraseña del administrador general; además, dicha contraseña debía ser resguardada en una caja fuerte.
- Cualquier cambio en la configuración del equipo tenía que ser autorizada y justificada; asimismo, debía ser específicamente documentada.
- Todos los usuarios debían ser monitoreados para conocer el uso de sus cuentas. Este monitoreo se llevaba a cabo de la siguiente manera:
  - Revisión de todas las bitácoras del sistema en un periodo máximo de un día.
  - Generación de 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 sólo el personal autorizado podía utilizarlo.

Asimismo, se establecieron reglas específicas:

- Asegurar que no se instalara 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, ya que podían ser un peligro latente para la seguridad e integridad del sistema.
- Se revisaban los mecanismos de autenticación entre los centros de procesamiento, tanto a nivel de equipo como 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.
- Los respaldos realizados en los equipos de cómputo eran completos. Fue necesario exportar la base de datos. Estos respaldos se hacían diariamente y en caso de que no se hicieran porque se estuviese utilizando el equipo, ya que no se podía dar de baja, se realizaba un respaldo compactado de las particiones principales.

Seguridad en la difusión

Para facilitar la información del PREP 2000 de manera oportuna, se pensó en que hubiera multiplicidad de sitios en donde ésta fuera publicada, de manera reiterada y actualizada periódicamente. Se tomó esta medida como prevención, ya que en caso de que se diera alguna alteración, en la siguiente actualización de los datos volvería a aparecer la información verdadera. La comunicación era unidireccional, es decir, desde los centros de procesamiento sólo se podía enviar la información actualizada hacia los centros de difusión, evitando así cualquier percance.

La multiplicidad de sitios y de vías a través de Internet evitaría la negación del acceso a las páginas que difundirían la información. Las firmas digitales con la información actualizada con una cierta periodicidad evitaba su alteración. Se señaló claramente en las páginas de difusión que la alteración de resultados electorales era delito que se castigaba con cárcel.

El hecho de introducir a Internet como medio de difusión tuvo como consecuencia la necesidad de proteger los equipos contra ataques, reforzando los esquemas de

seguridad que hasta el momento no se habían previsto: evitar cualquier intrusión o acceso no autorizado a los sistemas de información, y asegurar la disponibilidad o el acceso, uso de la información y recursos de cómputo cuando éstos eran requeridos. Todo se hizo con la integración de *firewall*, o sea, *softwar*e y/o *hardware* dedicados a proteger los servicios informáticos del PREP 2000.

La seguridad informática en la difusión se sustenta en forma importante en la correcta configuración de los elementos de la red, los servidores y la integración de *firewall*. Este sistema contaba con seguridad *multinivel*, su integridad no se basaba en un solo elemento, sino que era el resultado de unir configuraciones especiales en elementos de red, recorte de servicios en los equipos de cómputo, algoritmos de encripción y autenticación, aislamiento de la red institucional y control de acceso.

Se estableció un recorte de seguridad en los equipos de cómputo para asegurar que se utilizaran sólo los servicios y así evitar ataques en este sentido. Este mismo recorte se realizó para todos los elementos de red y se incorporaron en diferentes puntos de la misma.

La seguridad de los equipos de cómputo estuvo basada en dos vertientes: por un lado, considerando que todo contacto abierto con Internet es potencialmente poderoso, se destinaron equipos para cumplir la función de *firewall* o filtro de protección. Este elemento se configuró de manera que su dirección IP fuera invisible desde los equipos conectados en la red y así se evitaran ataques directos. Por el otro, se recortó el sistema operativo en todos los equipos, limitándolo a las rutinas estrictamente necesarias para los procesos electorales.

Además, se realizaron diversas auditorías de seguridad, comprobando la eficiencia de las medidas asumidas.

La prioridad dentro de la seguridad en comunicaciones fue la integridad y disponibilidad de los datos y la interconexión de las redes. En todos los dispositivos dentro de la red global del PREP 2000 se implementaron las medidas para garantizar su integridad y confiabilidad. Cuando una red no estaba bajo su administración, se consideraba insegura y se tomaron todas las precauciones para las conexiones a dichas redes.

Uno de los servidores que hacían posible la difusión recibía los datos del equipo de procesamiento y los preparaba para transmitirlos a los servidores de difusión *Web* internos que enviaban los datos a las salas de prensa, la red interna del IFE, redes de

partidos políticos y conteo rápido y de medios y proveedores de servicio de Internet (ISP). Para proteger la red de difusión de redes externas se utilizaron *firewall* que separaban las redes y controlaban el tráfico entre ellas.

La red del PREP 2000 no tuvo ninguna conexión directa a Internet, la difusión se realizó a través de los principales medios de comunicación, proveedores de servicios de Internet e instituciones educativas. Algunos medios redistribuyeron el paquete con la información a otros, considerados como un segundo nivel de difusión, y así se logró tener aproximadamente 28 sitios oficiales en Internet publicando los resultados del PREP 2000. Los archivos de difusión que eran enviados a los ISP estaban firmados con PGP para garantizar su autenticidad.

Acerca de la difusión el Dr. Enrique Daltabuit opina:

> Por seguridad se entiende que la información que se desea publicar se haga 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. Pero dada la legislación que tenemos y la forma en que se resolvió este posible problema, yo creo que el equipo del PREP 2000 hizo un trabajo excelente en la seguridad informática.