PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES (PREP)
PLAN DE SEGURIDAD OPERATIVA

ANEXO. I

Antecedentes

En el Proceso Electoral Estatal Ordinario 2017-2018, se contará con el Programa de Resultados Electorales Preliminares (PREP), el cual está sujeto a los Lineamientos del Programa de Resultados Electorales Preliminares, emitidos por Consejo General del Instituto Nacional Electoral aprobado con el Acuerdo No. INE/CG260/2014. En el diseño, instalación e implementación del PREP se deberá de cumplir con los principios de certeza, legalidad, independencia, imparcialidad, máxima publicidad y objetividad, en el ejercicio de la función electoral. Las disposiciones generales establecen en el artículo 5 la siguiente definición: "El PREP es el mecanismo de información electoral que recaba los resultados preliminares y no definitivos, de carácter estrictamente informativo a través de la captura de los datos asentados en las Actas de Escrutinio y Cómputo (AEC) de las casillas que se reciben en los Centros de Acopio y Transmisión de Datos (CATD) autorizados por el Instituto Electoral del Estado de Campeche (IEEC) en el ámbito de su competencia". Así mismo el artículo 6 de dichos lineamientos señala: "El PREP es un programa único, conformado por recursos humanos, materiales, procedimientos operativos, procedimientos de digitalización y publicación, seguridad y tecnologías de la información y comunicaciones, cuyas características, así como reglas de operación e implementación son emitidas por el IEEC a través de los presentes lineamientos con obligatoriedad para el propio IEEC. El IEEC es responsable directo de la implementación y operación del PREP, en el ámbito de sus competencias, así como de los recursos humanos, materiales, procedimientos operativos, procedimientos de seguridad y tecnologías de información y comunicaciones que establezcan con esos fines de conformidad con los presentes Lineamientos". Como parte de sus responsabilidades y funciones, el Comité Técnico Asesor, deberá de brindar asesoría técnica en materia de PREP en los ámbitos de su competencia, es por ello que en la 1ª. Sesión Ordinaria se estableció la Integración y propuesta del Plan de Trabajo para el Proceso Electoral Estatal Ordinario 2017-2018. En la 2ª Sesión Ordinaria llevada a cabo el día sábado 3 de enero de 2015, en el punto 15 de la Orden del Día se estableció que se deberá desarrollar el Plan de Seguridad con la finalidad de realizar el análisis de riesgos en materia de seguridad de la información que permita identificarlos y priorizarlos así como implementar los controles de seguridad aplicables en los distintos procesos del PREP, deberán de incluirse propuestas técnicas y estudios de factibilidad para adquisiciones, arrendamientos o integración de soluciones, que serán aplicables al entorno de infraestructura, hardware, software y acceso a aplicaciones. Los riesgos tendrán impacto al costo asociado, recursos humanos, áreas de amenazas, riesgos en caso de materializarse un ataque y plan de seguridad para resolver cada uno de los riesgos identificados.

Para tal efecto y dar cumplimiento a lo establecido en el punto 12 del Plan de Trabajo, el Comité Técnico Asesor, ha elaborado esta Propuesta de Plan de Seguridad que será utilizados para la Implementación del PREP que permitan contar con las mejores condiciones que garanticen llevar a cabo el Programa de Resultados Electorales Preliminares de acuerdo a los Lineamientos del Programa de Resultados Electorales Preliminares.

1. Generalidades

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas y organizaciones para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información. Estos riesgos que se enfrentan a llevado a que muchas desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a las organizaciones crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

Así mismo, y tal como lo define el Capítulo VI de Consideraciones de Seguridad Operativa de los Lineamientos del PREP, el correcto establecimiento del Plan de Seguridad permitirá llevar a cabo la implementación del control en los distintos procesos de operación del PREP, así como de la Infraestructura Tecnológica, basándose en los resultaos del análisis de riesgos en materia de seguridad de la información.

2. Objetivo

El objetivo de este documento, es cumplir con lo establecido en el Plan de Trabajo del Comité Técnico Asesor del PREP, que establece en el punto 12, la elaboración del Plan de Seguridad para la implementación del PREP.

3. Plan de Seguridad

3.1. Definición de Políticas de Seguridad

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.
No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y él por qué de ello, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.

Algunos conceptos que se aplican a la seguridad informática son confidencialidad, integridad, disponibilidad y Risk Management. El término Confidencialidad (Confidentiality) establece que la información sólo puede ser accedida por la persona y/o sistema con las credenciales pertinentes. Igualmente nadie sin credenciales puede tener acceso a ningún tipo de información dentro de la red. En la práctica, la confidencialidad se logra a través de la implementación del cifrado de la información. Debemos de cifrar tanto la información guardada en disco como la que viaja a través de la red. El término Integridad (Integrity) establece que la información NO puede ser modificada sin los permisos correspondientes, de lo contrario, la información es corrupta. La integridad de la información es lo que garantiza la validez de la información. En la práctica, para garantizar la integridad de la información se implementa algoritmos de Hashing. El término Disponibilidad (Availability) establece que la información debe de estar disponible a los usuarios de la red en el momento que se precise, de lo contrario, la red no cumple su cometido principal. Las redes pueden en algún momento no ofrecer servicio producto de un ataque informático, donde las peticiones de los usuarios legítimos NO son procesadas como consecuencia de una avalancha de acceso de manera simultánea proveniente desde el exterior. A esto se le llama Ataque de Negación de Servicios (Denial of Service Attack).

Por último, Algo que debemos tomar en cuanta antes de implementar cualquier política o solución de seguridad es realizar un estudio de Management Risk. ¿Qué es el Management Risk? Consiste es una estimación del valor de los activos de la empresa que necesitamos proteger de posibles amenazas. Los activos de una empresa pueden ser muy variados, pero en general entran en dos grandes categorías: tangibles e intangibles.

Los activos tangibles son lo que podemos tocar: PCs, tabletas, Smartphones, servidores, switch, router, dinero, personal, documentos, etc. Los activos intangibles son los que NO podemos tocar: propiedad intelectual, base de datos, archivos, patentes, bitcoins, etc.

El objetivo del Risk Management es evitar que la inversión en seguridad NO salga más cara que el activo a proteger. Por ejemplo, si tenemos una información que su costo de reposición —el tiempo estimado en recuperar la información en caso de pérdida— es de US$200.00, sería un crimen financiero invertir US$2,000.00 para proteger dicha información. Ahora bien, si tenemos una base de datos con la información de contacto de 500,000.00 clientes y el costo de reposición es de 2 millones, en un caso como este invertir US$20,000 en una solución de seguridad informática tiene mucho sentido financiero.

3.2. Elementos de la Política de Seguridad

Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la organización para lograr una visión conjunta de lo que se considera importante.

Las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Otro punto importante, es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

Por último, y no menos importante, el que las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etc.

3.3. Criterios de Evaluación de Riesgos

Se propone establecer la metodología OCTAVE Allegro pero personalizada como metodología de evaluación de riesgos en materia de seguridad informática para el proceso del PREP.

Este método establece que lo primero que deben realizar es el establecimiento del conjunto de criterios cualitativos con las cuales se podrá evaluar el efecto del riesgo del sistema PREP. Los criterios de evaluación de riesgos son los siguientes:

- Reputación/confianza de los ciudadanos sobre el PREP
- Entorno Político
- Seguridad/Salud
- Implicaciones Legales

Las áreas de impacto para cada categoría son las siguientes:

	Criterio de Medición de Riesgo: **Reputación/Confianza de los ciudadanos sobre el PREP**		
Área de Impacto	Bajo	Moderado	Alto
Certeza en los Resultados del PREP	Existe una discrepancia en la diferencia de resultados publicado vs las actas no mayor al 1%	Existe una discrepancia en la diferencia de resultados no mayor al 3%	Existe una discrepancia en la diferencia de resultados mayor al 3%
Publicación a Tiempo de los Resultados	La publicación de resultados tiene un retraso no mayor a 5 minutos en la	Existe un retraso no mayor a 30 minutos en la actualización de resultados	Caída en los sistemas de publicación de los Resultados, que no permite hacer la consulta

	actualización de los resultado		de los mismos
Afectación de la imagen del PREP	La información relacionada con incidente de seguridad se conoce dentro del área de TI	La información relacionada con incidente de seguridad se conoce dentro del IEEC	La información relacionada con incidente de seguridad se conoce públicamente

	Criterio de Medición de Riesgo: **Entorno Político**		
Área de Impacto	Bajo	Moderado	Alto
Consejeros Electorales	El incidente de seguridad es básico, no afecta al PREP y solo es conocido por el personal técnico del PREP.	El incidente de seguridad afecta parcialmente al PREP y es conocido sólo por el Presidente del IEEC.	El incidente de seguridad afecta gravemente al PREP y es conocido por la mayoría de los Consejeros Electorales
Partidos Políticos	El incidente de seguridad es básico, no afecta al PREP y solo es conocido por el personal técnico del PREP.	El incidente de seguridad afecta parcialmente al PREP y es probable que sea del conocimiento de algún partido político.	El incidente de seguridad afecta gravemente al PREP y es conocido por la mayoría de los Partidos Políticos.
INE	El incidente de seguridad es básico, no afecta al PREP, y no viola los Lineamientos del PREP.	El incidente de seguridad afecta parcialmente al PREP, además de que no se cumple con alguno de los Lineamientos del PREP.	El incidente de seguridad afecta gravemente al PREP, y además no se cumplen más de tres aspectos de los Lineamientos del PREP.

	Criterio de Medición de Riesgo: **Seguridad/Salud**		
Área de Impacto	Bajo	Moderado	Alto
Riesgo en la Vida de las personas que participarán en el PREP.	No hay pérdida de vidas humanas o amenazas significativas de las personas que participan en el PREP. No es necesario establecer ningún procedimiento legal	Existe un riesgo de pérdida de la vida de alguna persona, pero se recobra con tratamiento médico. Es posible que haya algún procedimiento legal ante el riesgo presentado.	Se pierde la vida de alguna persona, lo que desencadena procedimientos judiciales, así como altos costos económicos.
Salud de las personas que participarán en el PREP.	Se afecta la salud de forma mínima de alguna persona que participa en el PREP. La salud es recobrada totalmente a los pocos días	Se afecta la salud de forma temporal alguna persona que participa en el PREP. La recuperación de la salud puede tomar varios días o incluso semanas. Existen gastos relacionados con el tratamiento médico	Se afecta gravemente la salud de alguna persona que participa en el PREP, al punto de ser permanente o que pueda tomar varias semanas o meses en recuperar. Existen altos costos de tratamiento médico, y se pueden presentar

			demandas legales.
Seguridad Física y Ambiental	La seguridad física del Recinto Central o de los CATDs se ve comprometida mínima. No se requiere presentar demandas legales, y las afectaciones económicas son de bajo costo (menores a $10,000.00).	La seguridad física del Recinto Central o de los CATDs se ve afectada. Es posible que se requiere presentar demandas legales, y las afectaciones económicas son inferiores a los $100,000.00 pesos.	Se presenta una violación grave a la seguridad física del Recinto Central o de los CATDs. Es obligado que se presente demandas legales así como investigaciones por las autoridades competentes. Se generan gastos superiores a los $100,000.00

	Criterio de Medición de Riesgo: **Implicaciones Legales**		
Área de Impacto	Bajo	Moderado	Alto
Multas	El incidente de seguridad generan multas menores a $1,000.00	El incidente de seguridad generan multas menores a $10,000.00	El incidente de seguridad generan multas superiores a $10,000.00
Demandas	Existe el riesgo de una demanda, generada por algún incidente de seguridad.	Se presenta una demanda generada por el incidente de seguridad, y además genera gastos económicos inferiores a los $10,000.00. Existe el riesgo de la inhabilitación de un funcionario relacionado con el PREP.	Se presenta un incidente grave de seguridad, que genera una demanda, que pudiera generarse acciones penales. Además de generaron gastos económicos superiores a los $10,000.00. Existe la inhabilitación de algún funcionario relacionado con el PREP.
Acciones Penales	Se genera un riesgo de alguna acción penal, sin que la gravedad amerite la privación de la libertad.	Se genera un incidente de seguridad que desencadena en una acción penal.	Se genera un incidente grave de seguridad, que provoca la aprehensión de alguna persona relacionada con el PREP.

3.4. Activos Críticos

En este punto, nos hemos dado a la tarea de identificar los recursos humanos y materias, servicios e información que son críticos para el proceso del PREP, tomando en consideración los Criterios de Medición de Riesgos establecidos en el punto anterior. A continuación se enlistan:

- Sistema Informático del PREP.
- Servidores de Red
- Enlace de Telecomunicaciones Telmex Recinto Central (recepción digitalizada de AEC de los CATD)
- Enlace a Internet para la publicación de resultados
- Enlaces Infinitum de los CATD (envío de las AEC digitalizada)
- Auditores Externos
- Personal Técnico del Sistema Informático PREP.

- Computadoras de Captura de Información
- Escáner de imágenes para Digitalización de Actas
- Sitios Web de los Difusores
- Video proyectores de la Salas de Proyección de Resultados
- Personal Operativo que operar el sistema informático del PREP.

3.5. Áreas de Amenaza

De manera enumerativa se identifican y clasifican las siguientes áreas de amenaza:

- Centro de Acopio y Transmisión de Datos
- Recinto Central
- Enlaces de Telecomunicaciones
- Mecanismos de Difusión

3.6. Identificación de Riesgos

Los riesgos que se han identificado son los siguientes:

- Robo de Equipo y sabotaje
- Denegación del Servicio
- Manejo de Código Malicioso en el Sistema Informático
- Acceso no autorizado de personas ajenas al proceso
- Caída en el enlace principal del Recinto Central
- Caída en los servidores de aplicativo (sistema informático del PREP) y bases de datos
- Caída en el suministro de energía eléctrica que ofrece CFE
- Fallas en las computadoras de captura de información
- Fallas en los Escáneres
- Que no se presente el personal operativo de captura de la información del PREP.

3.7. Plan de Seguridad (Acciones del Plan)

El Plan de Seguridad lo hemos dividido en los siguientes puntos:

- Robustecimiento de los proceso Operativos
- Fortalecimiento de la Infraestructura Tecnológica
- Seguridad en la Captura
- Seguridad en el Recinto Central
- Seguridad en la Transmisión
- Seguridad en el Procesamiento
- Seguridad en la Publicación
- Robustecimiento de los Controles de Seguridad Física y Ambiental
- Creación del Plan de Continuidad

3.7.1. Robustecimiento de los procesos Operativos

La formulación de la estrategia de protección se va a enfocar tanto en los aspectos tecnológicos, como en los procesos que conforman la operación, integrando de esta manera una visión completa de la seguridad de la información procesada.

Se debe de contar con los controles administrativos (procedimientos, manuales y/o instructivos) requeridos para la operación del PREP. Estos procedimientos deben de estar alineados con el Análisis de Riesgos detectados en los puntos del 4.3 al 4.6 de este Plan de Seguridad.

En apego a las mejores prácticas en la materia se detalle la matriz que lista todos los controles de seguridad identificados que deben ser desarrollados por el área de tecnologías del IEEC:

- Respaldos de Información
- Protección de llaves criptográficas
- Monitoreo de sistemas, equipos y aplicativos
- Atención a Incidencias de seguridad incluyendo:
    - Robo de Equipo y/o sabotaje
    - Denegación de Servicio
    - Manejo de Código Malicioso
    - Acceso no autorizado

3.7.2. Fortalecimiento de la Infraestructura Tecnológica

Se propone el fortalecimiento de la Infraestructura Tecnológica, particularmente aquella que hemos detectado en los puntos 4.4 y 4.5. En lo relativo al fortalecimiento de los Activos Críticos, se deben de considerar al menos lo siguiente:

- Sistema Informático del PREP. De acuerdo al diagnóstico y dictamen técnico elaborado por el Comité Técnico Asesor del PREP del Instituto Electoral del Estado de Campeche, se determinó que la alternativa adecuada para la implementación y operación del PREP, se lleve a cabo por medio de la contratación de un tercero. Para tal efecto, y dada la importancia de contar con un proveedor que garantice cumplir a cabalidad todos los puntos referidos en los Lineamientos, se deberá de efectuar la contratación de un proveedor con amplia experiencia en PREP, utilizando un mecanismo de evaluación que contenga las variables de capacidad técnica, solvencia económica, experiencia, especialidad y cumplimiento de contratos.
- Servidores de Red. Este punto de infraestructura es crucial, por lo tanto se deberá de considerar que se adquieran Servidores de alta desempeño para la instalación del Sistema Informático en un arquitectura paralela con un mecanismo de balanceo de cargas, de tal forma que cada servidor pueda atender las peticiones por parte de los usuarios del Recinto Central, como de los CATD. En lo relativo a las comunicaciones se sugiere que los servidores se conecten a los switches a través de puertos a 10 GbE, y que los puertos asignados de los switches asignados a los servidores sólo puedan gestionar tráfico relativo a peticiones realizadas a los servidores.
- Enlace de Telecomunicaciones Telmex Recinto Central (recepción digitalizada de AEC de los CATD). En la Sede del Consejo General del IEEC se cuenta con un servicio de Carrier de Fibra Óptica suministrada por Telmex con un ancho de banda de 10 Mb de entrada y salida. En el caso de que la sede que servirá para el Recinto Central se encuentre a una distancia muy cercana a las oficinas del IEEC como se ha propuesto, se propone utilizar el canal de telecomunicaciones para atender las necesidades de comunicación del Recinto Central. Sin embargo, será necesario contar con un enlace de telecomunicaciones adicional para contar con un canal redundante de comunicaciones ante un eventual fallo en el enlace principal con que contará el IEEC en la jornada electoral.
- Enlace a Internet para la publicación de resultados. De igual forma que en el punto anterior, se pretender utilizar el servicio de Carrier de Fibra Óptica como canal de telecomunicación principal, será necesario contar con un enlace de telecomunicaciones adicional para contar con un canal redundante de comunicaciones ante un eventual fallo en el enlace principal con que contará el IEEC en la jornada electoral.
- Enlaces Infinitum de los CATD (envío de las AEC digitalizada). En las sedes que se ocuparán como los CATD, es difícil que se cuente con la posibilidad de contar con canales alternativos de comunicación fijos, sin embargo, en aquellos lugares donde los proveedores de telefonía móvil (Telcel, Iusacell, Movistar, etc.) ofrezcan servicios de transmisión de datos, se deberá de contratar los dispositivos de Banda Ancha Móvil (BAM) con el crédito suficiente, como mecanismos alternativo de transmisión de datos. Es importante considerar la cantidad de actas a transmitir en cada CATD, para

calcular el contar con el crédito suficiente en el paquete de datos, que permita transmitir al menos tres veces la cantidad en Mb, de información.

- Auditores Externos. Tal como lo establece el artículo 34 de los Lineamientos los responsables de llevar a cabo la Auditoría deberán de contar con experiencia en auditoría de sistemas, así mismo señala que se deberá dar preferencia a instituciones académicas o de investigación, con reconocimiento nacional o internacional. En el documento de Propuesta de Procedimiento de Auditoría se estableció que se hizo un análisis de aquellas instituciones que cuentan con personal con experiencia o áreas de investigación relacionadas con las tecnologías de información, así como con la conveniencia de la ubicación física de dichas instituciones que nos permitan abaratar costos de traslados, estancias, transportación de personal y equipos tecnológicos, y se propuso que los responsables de la Auditoría, puedan ser alguna de las siguientes instituciones académicas del estado de Campeche: la Facultad de Ingeniería y/o Dirección de Tecnologías de Información de la Universidad Autónoma de Campeche (UAC); la Facultad de Tecnologías de Información y/o Coordinación General de Tecnologías de la Información y la Comunicación de la Universidad Autónoma del Carmen (UNACAR); el Instituto Tecnológico de Campeche; el Instituto Tecnológico Superior de Calkiní (ITESCAM) la Universidad Interamericana para el Desarrollo (UNID).
- Personal Técnico del Sistema Informático PREP. Se propone que al contratar al proveedor del PREP, se asegure de contar con personal técnico de apoyo a lo largo de la jornada electoral. Este personal NO estará a cargo de operar el Sistema del PREP, sino solamente en labores de apoyo para restablecer el sistema informático en caso de alguna eventualidad.

3.7.3. Seguridad en la Captura

Se deberán de establecer los controles necesarios para brindar un alto grado de seguridad al propio proceso de captura de las Actas PREP, entre los que se proponen los siguientes:

- Para habilitar cualquier computadora de captura de información, será necesario que tanto el Coordinador, el Supervisor y el Capturista se registren con su nombre de usuario y contraseña única.
- El sistema informático deberá de considerar una doble captura de los datos, reduciendo así la posibilidad de errores humanos. Adicionalmente, un verificador deberá de verificar y cotejar que los datos capturados en el sistema informático coincidan con la información plasmada en el AEC, además de verificar que la imagen publicada del AEC corresponda a la casilla en cuestión, por medio de una revisión del encabezado del AEC con respecto a la imagen publicada.
- Se debe de asegurar que las computadoras de captura de información cuenten con las capacidades necesarias para almacenar todas las transacciones que se generaron en dicha computadora. Esto tiene dos propósitos: por una parte tener la posibilidad de hacer una retransmisión de todo lo registrado y/o capturado en caso de una contingencia en el Recinto Central, y por otro lado que las transacciones queden almacenadas para posibles auditorías posteriores al día de la Jornada Electoral.
- La autenticidad e integridad de cada una de las transacciones que sean enviadas al centro de cómputo estén protegidas mediante la aplicación de técnicas criptográficas con llaves de 192 bits, utilizando el estándar “Advanced Encryption Standard” (AES).

3.7.4. Seguridad en el Recinto Central

Se debe de contar con las siguientes medidas de seguridad en el Recinto Central que evite un comportamiento anormal del sistema de información:

- Se debe de contar con un enlace de telecomunicaciones adicional al que ya cuenta el IEEC.

- Se debe de contar con servidores de alto desempeño con una configuración en un arquitectura paralela con un mecanismo de balanceo de cargas, de tal forma que cada servidor pueda atender las peticiones por parte tanto de los usuarios del Recinto Central, como de los CATD
- Se debe de contar con una planta de emergencia de energía eléctrica con una capacidad suficiente para soportar la carga de energía de todo el Recinto Central, no solo de los servidores, computadoras y demás equipos de telecomunicaciones, sino también del alumbrado público y otros servicios que requieren de energía eléctrica.
- Se debe contar con una solución de almacenamiento masivo de información que permita salvaguardar la información generada en el sistema informático del PREP.
- Se debe de contar con equipos de cómputo adicional que puedan ser utilizadas como equipos de respaldo en caso de fallo de alguno de los equipos de cómputo de captura.

3.7.5. Seguridad en la Transmisión

Dentro de los equipos de comunicaciones con tareas específicas de seguridad de la información, se deberá de contar con los siguientes equipos y/o dispositivos:

- Uso de dispositivos de detección de intrusos a nivel de red, configurados y ajustados de acuerdo al tráfico que se espera en el centro de cómputo
- Uso de dispositivos de filtrado de paquetes de red (Firewalls) para proteger el perímetro de la infraestructura tecnológica del Recinto Central. Cabe mencionar que se deberá de establecer una política restrictiva para configurar los dispositivos de filtrado, esto es se debe de restringir todo el acceso de tráfico a la red del Recinto Central y solamente se deberá de habilitar el acceso a aquellos puertos que sean estrictamente necesarios.
- Se debe de contar con equipos redundantes para los dos casos señalados en los puntos anteriores del tal forma que se tenga un esquema de redundancia para garantizar que el tráfico estará siendo analizado por los dispositivos mencionados.

En lo relativo a la conectividad, se deberán tener en cuenta las siguientes consideraciones relativas a la Seguridad Informática:

- El diseño topológico deberá de estar orientado a brindar alta disponibilidad
- Se debe de hacer una segmentación del tráfico de las diferentes capas de procesamiento de la información usando redes virtuales
- La información solamente debe de viajar desde los CATD hacia el Recinto Central. Nunca en sentido contrario. La configuración de reglas de acceso en todos los dispositivos de comunicaciones deben de seguir este principio.
- Se propone contar con un esquema de monitoreo proactivo de todos los enlaces de red. El centro de monitoreo podrá estar ubicado dentro del Centro de Cómputo y/o el Centro de Operaciones del IEEC.
- La configuración de todos los dispositivos de comunicaciones involucrados (switches, routers, y firewalls) deberán de tomar como base las recomendaciones de seguridad de organismos reconocidos internacionalmente en la materia como el Instituto Nacional de Estándares y Tecnologías (NIST).

3.7.6. Seguridad en el Procesamiento

En el rubro de servidores de aplicación se proponen las siguientes consideraciones respecto a la Seguridad Informática:

- Para garantizar la alta disponibilidad del aplicativo se debe de implantar una arquitectura paralela distribuida de servidores, interconectados entre sí. Mediante un mecanismo de balanceo de carga, cada servidor debe de tener la posibilidad de atender peticiones por parte de los CATD.
- Cada servidor deberá de contar con un sistema operativo especialmente para servidores de aplicaciones como puede ser Windows Server Enterprise Edition, Linux RedHat AS 4.0 entre otros.

De manera adicional se propone que se habiliten opciones para reforzar la seguridad a nivel del núcleo del sistema

- En el rubro de control de acceso, cabe mencionar que las reglas de control de tráfico que fueron aplicadas a nivel de dispositivos de comunicaciones fueron también configuradas a nivel de sistema operativo. Cada servidor procesó única y exclusivamente el tráfico que se consideró esperado.

En lo relativo a la capa de servidores de bases de datos se tiene que poner mucha atención, ya que la primera etapa de la estrategia de recuperación en caso de desastres estará basada en la correcta replicación de los datos entre el servidor de base de datos primario y el secundario, mismos que estarán instalados en el Centro de Cómputo del IEEC. En este sentido, se deberán de tomar en cuenta las siguientes previsiones:

- Uso de tecnología de manejadores de base de datos (SQL Server, Oracle, etc) para garantizar la alta disponibilidad y la correcta réplica de información entre los servidores de bases de datos del Centro de Cómputo.
- Se sugiere el uso de tecnología de virtualización VMWare para facilitar el aprovisionamiento de escenarios de desarrollo y pruebas del sistema
- Adicional al control de acceso a nivel de sistema operativo, se deberán de aplicar los ajustes necesarios para que el manejador de la base de datos restringiera el acceso solamente a los usuarios autorizados.
- Se debe de contar con un sistema de monitoreo proactivo, que permitió conocer en todo momento el estado de la base de datos.

El mecanismo para almacenamiento de datos es crítico para el correcto funcionamiento de todo el programa, por lo que se debe de considerar una red de almacenamiento (Storage Area Network) para brindar el nivel de certeza requerido. La configuración de la SAN debe considerar también elementos de seguridad informática, como los que se proponen a continuación:

- Red independiente, dedicada al almacenamiento, basada en la tecnología Fibre Channel
- Redundancia de los switches, asegurando así alta disponibilidad
- Balanceo de carga a nivel de servidor
- La configuración de la SAN debe de contemplar las mejores prácticas de seguridad referidas por organismos a nivel mundial

Adicionalmente a los elementos expuestos, se sugiere la contratación e implantación de un “Security Operation Center” (SOC), el cual estaría conformado por un equipo de monitoreo-respuesta que esté integrado por personal especializado que lleve a cabo en tiempo real el análisis de los posibles incidentes de seguridad informática que llegaran a presentarse. Éste deberá de estar de manera constante en coordinación con áreas internas y externas para tomar las acciones pertinentes.

3.7.7. Seguridad en la Publicación

Tal como se establece en los Lineamientos, la divulgación de los resultados electorales preliminares, se llevará a cabo a través del propio IEEC, así como a través de Difusores oficiales, que apoyaran con la publicación de información a través de sus correspondientes portales de Internet.

Los mecanismos de seguridad informática que se deberán implantar en este rubro consistirán en firewalls para protección del perímetro y la definición de un protocolo de transferencia de información en un solo sentido: del IEEC hacia los diversos medios. La conexión a los medios se propone que se realice a través de enlaces de comunicación dedicados, mediante los cuales se depositarán archivos en un equipo dedicado del difusor.

3.7.8. Robustecimiento de los Controles de Seguridad Física y Ambiental.

La seguridad física es un factor crítico para garantizar que la seguridad de la información no se vea afectada, ya sea por daño físico o por configuraciones realizadas por personal no autorizado. De igual forma se debe poner especial atención a los factores ambientales tales como: condiciones de humedad, aire acondicionado, filtros de polvo, sensores de incendio, alimentación eléctrica, etc.

En este sentido se proponen las medidas necesarias para garantizar la seguridad física y ambiental basadas en los resultados del Análisis de Riesgos y en los controles que presenta el estándar internacional de seguridad informática.

Tomando en consideración el Diagnóstico elaborado por el Comité Técnico Asesor, así como las visitas que se han efectuado a las sedes que albergarán a los CATD para evaluar la seguridad física y ambiental, se deberá de considerar los siguientes elementos que mitiguen los riesgos en la seguridad física y ambiental:

- Seguridad en el Centro de Cómputo, así como el edificio que albergará el Recinto Central.
- Sistema de Control de Acceso para el Centro de Computo, el Recinto Central y los CATD
- Equipo de CCTV (Circuito Cerrado de Televisión) tanto en el Centro de Computo y el Recinto Central, y de preferencia también en los CATD
- Controles Ambientales
- Protección de Equipo e Información Sensible
- Seguridad Perimetral en el Centro de Cómputo, así como en cada uno de los CATD
- Sistema de Detección de Intrusos en el Centro de Cómputo.

A partir del diagnóstico se deberán considerar las actividades de corto plazo, mediano plazo y largo plazo, de tal manera general, que se lleve a cabo la implementación de controles para garantizar la seguridad en los siguientes rubros:

- Establecimiento de personal de seguridad para el control de acceso al Centro del Cómputo, así como del Recinto Central, y de los CATD
- Registro del personal que accedió al Centro de Cómputo
- Limitación de acceso solo para personal autorizado
- Establecimiento de medidas preventivas de contingencia
- Suministros de energía redundantes dentro del Centro de Cómputo para activos críticos
- Revisiones y mantenimiento hacia los servidores que servirán como servidores de aplicaciones y base de datos.
- Separación adecuada de los cables de datos con los cables de energía eléctrica
- Protección contra intercepción y estática del cableado de los datos y energía eléctrica
- Establecimiento del personal de mantenimiento de los servidores y equipos dentro del Centro de Cómputo
- Almacenaje adecuado de la información y medios removibles de forma segura
- Protección para las áreas de carga y descarga
- Sistemas de detección de humo y extinción de incendios en el Centro de Cómputo, así como el Recinto Central.

3.7.9. Creación del Plan de Continuidad

Como lo estable el artículo 40 de los Lineamientos, y dar cumplimiento a lo establecido en el punto 13 del Plan de Trabajo, el Comité Técnico Asesor, deberá de elaborar un programa denominado Plan de Continuidad que determine acciones que garanticen las ejecuciones de los procesos de acopio, digitalización, captura, verificación y publicación en caso de que se suscite una situación adversa o de contingencia. En lo que

respecta a nuestro Plan de Seguridad se deberá de documentar, implementar y probar un Plan de Continuidad que considere la continuidad de los procesos críticos por medio de un BCP (Business Continuity Planning) así como la recuperación de la tecnología que soporta dichos procesos por medio de un DRP (Disaster Recovery Planning).

El Plan de Continuidad deberá plantear como objetivo el detectar los riesgos presentes, analizar su probabilidad de ocurrencia, establecer su criticidad según cómo afectan la continuidad de los servicios, considerando los escenarios de contingencia (desastre total o desastre parcial) que pudieran afectar a los servicios informáticos a nivel nacional.

Las metas para la recuperación en caso de desastre deberán incluir los siguientes puntos:

- La recuperación de los servicios soportados en el Centro de Cómputo del IEEC ubicado en las Oficinas General del IEEC.
- Proporcionar los elementos para restablecer los servicios informáticos durante la vida del PREP.
- Detectar las interrupciones de los sistemas de una manera oportuna
- Crear una estrategia de respuesta y recuperación que asegure la restauración oportuna
- Minimizar las pérdidas y daños inmediatos

Adicionalmente será necesario determinar con los responsables del Sistema Informático del PREP los tiempos de recuperación y tolerancia de la aplicación, y validar que estos tiempos, sean acordes a los requerimientos de operación del PREP.

5. Conclusiones y Recomendaciones

5.1. Conclusiones

El plan de Seguridad que hemos detallado en este documento, se ha elaborado tomando como base los resultados del análisis de riesgos en materia de seguridad, que permita hacer una implementación exitosa de la operación del PREP. En la elaboración de este Plan tomamos como base la metodología OCTAVE Allegro pero personalizada como metodología de evaluación de riesgos en materia de seguridad informática para el proceso del PREP. De esta metodología se identificaron los activos críticos, las áreas de riesgo, así como los principales riesgos que pudieran presentarse en la operación del PREP, durante la jornada electoral.

Los activos críticos que se detectaron son el Sistema Informático del PREP, los Servidores de Red (tanto de Aplicaciones como de Base de Datos), el Enlace de Telecomunicaciones Telmex Recinto Central (recepción digitalizada de AEC de los CATD), el Enlace a Internet para la publicación de resultados, los Enlaces Infinitum de los CATD (envío de las AEC digitalizada), los Auditores Externos, el Personal Técnico del Sistema Informático PREP, las computadoras de Captura de Información, los Escáneres de imágenes para Digitalización de Actas, los Sitios Web de los Difusores, los Video proyectores de la Salas de Proyección de Resultados y finalmente el Personal Operativo que registrará la información en el sistema informático del PREP. En la parte de áreas críticas se detectaron las siguientes: el Centro de Acopio y Transmisión de Datos, el Recinto Central, los Enlaces de Telecomunicaciones así como los Mecanismos de Difusión.

Entre los principales riesgos encontramos el Robo de Equipo y sabotaje, la Denegación del Servicio, el Manejo de Código Malicioso en el Sistema Informático, el Acceso no autorizado de personas ajenas al proceso, la Caída en el enlace principal del Recinto Central, la Caída en los servidores de aplicativo (sistema informático del PREP) y bases de datos, la Caída en el suministro de energía eléctrica que ofrece CFE, las posibles fallas en las computadoras de captura de información, las posibles fallas en los Escáneres así como que no se presente el personal operativo de captura de la información del PREP en la jornada electoral.

Una vez que se hizo el Análisis de Riesgos, se elaboró el Plan de Seguridad que establece las acciones a seguir que atiende que atiende a los puntos detectados en el análisis de riesgos. El plan se dividió en los puntos: Robustecimiento de los proceso Operativos, Fortalecimiento de la Infraestructura Tecnológica, Seguridad en la Captura, Seguridad en el Recinto Central, Seguridad en la Transmisión, Seguridad en el Procesamiento, Seguridad en la Publicación, Robustecimiento de los Controles de Seguridad Física y Ambiental y finalmente la Creación del Plan de Continuidad.

5.2. Recomendaciones

Las recomendaciones que se hacen en referencia al Plan de Seguridad se detallan a continuación:

- Se deberá de considerar en el Presupuesto de Gastos del Instituto Electoral del Estado de Campeche, la inversión en las acciones que componen este Plan de Seguridad, a fin de asegurar que se cumple el objetivo de la elaboración de dicho Plan.
- El funcionamiento del Plan de Seguridad y alcance de este Plan de Seguridad, dependerá del grado de implementación de las acciones establecidas.
- Es imprescindible el fortalecimiento de la Infraestructura Tecnológica, para atender este Plan, pues para garantizar la continuidad del proceso del PREP durante la jornada electoral, se requiere contar con equipamiento tecnológico en configuraciones de redundancia así como con equipamiento de pueda servir como respaldo y/o soporte, ante posibles contingencias. Es particularmente importante el contar con Servidores de Alto Desempeño que serán usados para el PREP, y que al término de la jornada podrán ser usados para otras actividades dentro del IECC. Así mismo, se requiere la adquisición de algún sistema de almacenamiento masivo de información que permita almacenar la información del proceso del PREP ya sea para fines de auditorías que posteriormente se pudieran requerirse, o para fines estadísticos o históricos.
- El Plan de Continuidad deberá tomar como base los aspectos establecidos en el Plan de Seguridad, y deberá de estar alineado al mismo. El Plan de Continuidad deberá incluir desde aspectos básicos como el restablecimiento de las operaciones ante problemas con el suministro de energía eléctrica como situaciones catastróficas como pueden ser incendios, inundaciones, etc. En este Plan de Continuidad deberá detallarse claramente quienes son los responsables de activar el Plan, así como los recursos involucrados, deberá también de especificarse los criterios de activación del plan, y los tiempos en los cuáles será ejecutado.