INSTITUTO ELECTORAL DEL ESTADO DE ZACATECAS

ORGANISMO PÚBLICO LOCAL ELECTORAL

Plan de Seguridad del Programa de Resultados Electorales Preliminares para la elección de Diputados y Ayuntamientos en el Proceso Electoral Local 2017-2018.

Zacatecas

PROCESO ELECTORAL LOCAL

2017 | 2018

Contenido

Plan de Seguridad del Programa de Resultados Electorales Preliminares para la elección Diputados y Ayuntamientos en el Proceso Electoral Local 2017-2018.

I. Introducción

Un Plan de seguridad permite llevar a cabo la implementación de controles en los distintos procedimientos, en este caso, de operación del PREP, así como en la infraestructura tecnológica.

Las políticas de seguridad informática surgen como una herramienta organizacional para concientizar sobre la importancia y sensibilidad de la información y servicios críticos. 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 institución.

Algunos conceptos que aplican a la seguridad informática son confidencialidad, integridad, disponibilidad y manejo de riesgos. El termino confidencialidad establece que la información solo 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. El termino integridad establece que la información no puede ser modificada sin los permisos correspondientes, de lo contrario, la información es corrupta. La integridad de la información garantiza la validez de la información. El termino disponibilidad establece que la información debe estar disponible a los usuarios de la red en el momento que se precise, de lo contrario, la red no cumple su cometido principal. Por último, algo que se debe tomar en cuenta antes de implementar cualquier política de seguridad es estimar el valor de los activos de la institución que necesitamos proteger de las posibles amenazas.

II. Definiciones

IEEZ Instituto Electoral del Estado de Zacatecas
PREP Programa de Resultados Electorales Preliminares
CATD Centros de Acopio y Transmisión de Datos del PREP
CCV Centro de Captura y Verificación
CE Consejo Electoral Distrital/Municipal del IEEZ
CEsCo Centro Estatal de Cómputo
CEsCoRes Centro Estatal de Cómputo de Respaldo
DESI Dirección Ejecutiva de Sistemas Informáticos
AEC Actas de Escrutinio y Cómputo

PREP-Casilla Aplicación que permite la captura de la imagen del AEC desde casilla

III. Alcance

Todos los involucrados directa o indirectamente en la ejecución e implementación del Programa de Resultados Electorales Preliminares (PREP)

IV. Responsable

Dirección Ejecutiva de Sistemas Informáticos

V. Marco Jurídico

Reglamento de Elecciones del Instituto Nacional Electoral.
Anexo 13. Lineamientos del PREP

“

Capítulo IV
Consideraciones de Seguridad Operativa

12. Para la implementación de los controles de seguridad aplicables en los distintos procedimientos del PREP, se considerarán como mínimo los siguientes puntos:

VI. Plan de seguridad: Se deberá elaborar un plan de seguridad basado en los resultados de la estrategia de gestión de riesgos, que permita llevar a cabo la implementación de controles en los distintos procedimientos de operación del PREP, así como en la infraestructura tecnológica. ”

VI. Activos críticos

A continuación se enlistan los activos críticos para el proceso PREP, tomando en consideración los riesgos identificados por la DESI.

- Sistemas informáticos PREP
- Servidores web y de bases de datos en centro de datos principal y secundario
- Equipo de telecomunicaciones, en CATD, en CCV y en centros de datos principal y secundario
- Enlaces de telecomunicaciones a CESCo, centro de datos secundario

- Enlaces de internet de los CATD y CCV
- Personal PREP
- Computadoras para captura, digitalización, verificación y publicación PREP
- Escaners para digitalizar actas y para leer el código de barras
- Dispositivos móviles para digitalizar actas desde casilla
- Sitio web para difundir en internet los resultados
- Pantallas para publicar resultados en la sala del Consejo General

VII. Identificación de Riesgos

Con base en un análisis efectuado por la DESI se enlista la siguiente tabla que contiene 41 riesgos:

No.	Riesgo que acontece
1	No es posible identificar a que casilla corresponde el acta
2	La información de las AEC es capturada con errores
3	Las AEC son dañadas por el escáner
4	No puede llevarse a cabo el proceso de digitalización del AEC
5	No puede llevarse a cabo la captura de la imagen del AEC desde la casilla por no existir suficiente iluminación
6	Las configuraciones de los equipos en los CATD´s o CCV son modificadas por error o intencionalmente
7	El equipo se daña, por descuido, fin de vida útil en algún componente o intencionalmente
8	El dispositivo móvil se daña, por descuido, fin de vida útil en algún componente o intencionalmente
9	El equipo de cómputo tiene un funcionamiento distinto al esperado
10	El dispositivo móvil tiene un funcionamiento distinto al esperado
11	El equipo es sustraído del CATD o CCV
12	El dispositivo móvil es sustraído
13	Los CATD, CCV y el CEsCo quedan imposibilitados para transmitir y recibir información entre los dispositivos interconectados y los servidores
14	La aplicación móvil no transmite las imágenes de AEC capturadas desde casilla
15	Los servidores se dañan, colapsan o tienen un funcionamiento distinto al esperado, provocando que se detenga el avance en el procesamiento y difusión de resultados preliminares
16	Los servidores quedan expuestos a la alteración, modificación y/o destrucción de la información, así como a un daño intencional
17	El equipo de comunicación se daña por fin de vida útil en algún componente
18	Las pantallas para proyección de resultados PREP en la sala de sesiones del Consejo General presentan fallas de energía eléctrica y/ o tienen un

No.	Riesgo que acontece
	funcionamiento distinto al esperado
19	Incremento en el número de actas mal capturadas o identificadas con inconsistencias
20	Exposición de información confidencial hacia personas ajenas al procedimiento
21	El almacenamiento y respaldo de la información en la base de datos principal se interrumpen
22	El equipo para conectarse a la red privada se daña y no permite establecer la comunicación con el Centro de datos principal
23	La aplicación para transmitir y recibir información en los CATD o CCV, tiene un funcionamiento distinto al esperado
24	La solución informática para brindar protección a los servidores virtuales del PREP se daña, dejando vulnerable los equipos
25	Impedimento para visualizar la información de los resultados preliminares en el portal principal de publicación PREP
26	Los servicios de comunicación utilizados para transmitir y recibir información se interrumpen
27	Difundir información incorrecta en el portal de internet
28	Equipo vulnerable ante la presencia de personal ajeno al PREP en los CATD
29	CATD, CCV o el CEsCo presenta fallas en la energía eléctrica
30	Un desastre natural ocasiona fallas al Centro de datos principal donde se almacena y procesa la información del PREP
31	El funcionario se encuentra imposibilitado para realizar las actividades que tienen encomendadas (acopio, doble captura, digitalización, validación y supervisión)
32	Personal PREP es obligado a realizar actividades ajenas al PREP
33	Los equipos de suministro y generación de energía secundarios se dañan intencionalmente, por descuido, falta de mantenimiento o por fin de vida útil en algún componente
34	El cableado eléctrico o de datos se dañan y se imposibilita su uso
35	En los servidores para publicar en internet se detectan ataques
36	Personal PREP se retira del CATD antes de terminar de capturar, digitalizar, verificar y publicar las actas de escrutinio y cómputo
37	La mica utilizada para escanear actas se daña
38	En caso de fallo del sistema informático central
39	En caso de falta de enlaces de telecomunicaciones
40	Personal PREP no se presenta el día de la Jornada Electoral
41	En caso de un desastre natural o acto vandálico

VIII. Plan de Seguridad

En atención a los riesgos identificados y a los activos críticos se plantea el plan de seguridad de acuerdo a los siguientes rubros:

- Políticas de seguridad para el uso de los equipos de cómputo instalados en los CATD y CCV para la implementación del PREP
- Políticas de Seguridad para el uso de dispositivos móviles que serán empleados para la implementación del PREP-casilla
- Políticas de seguridad del centro de datos
- Seguridad en la transmisión de datos
- Infraestructura tecnológica
- Seguridad en la captura
- Seguridad en la publicación
- Controles de seguridad física y ambiental
- Seguridad de la energía eléctrica
- Plan de Continuidad

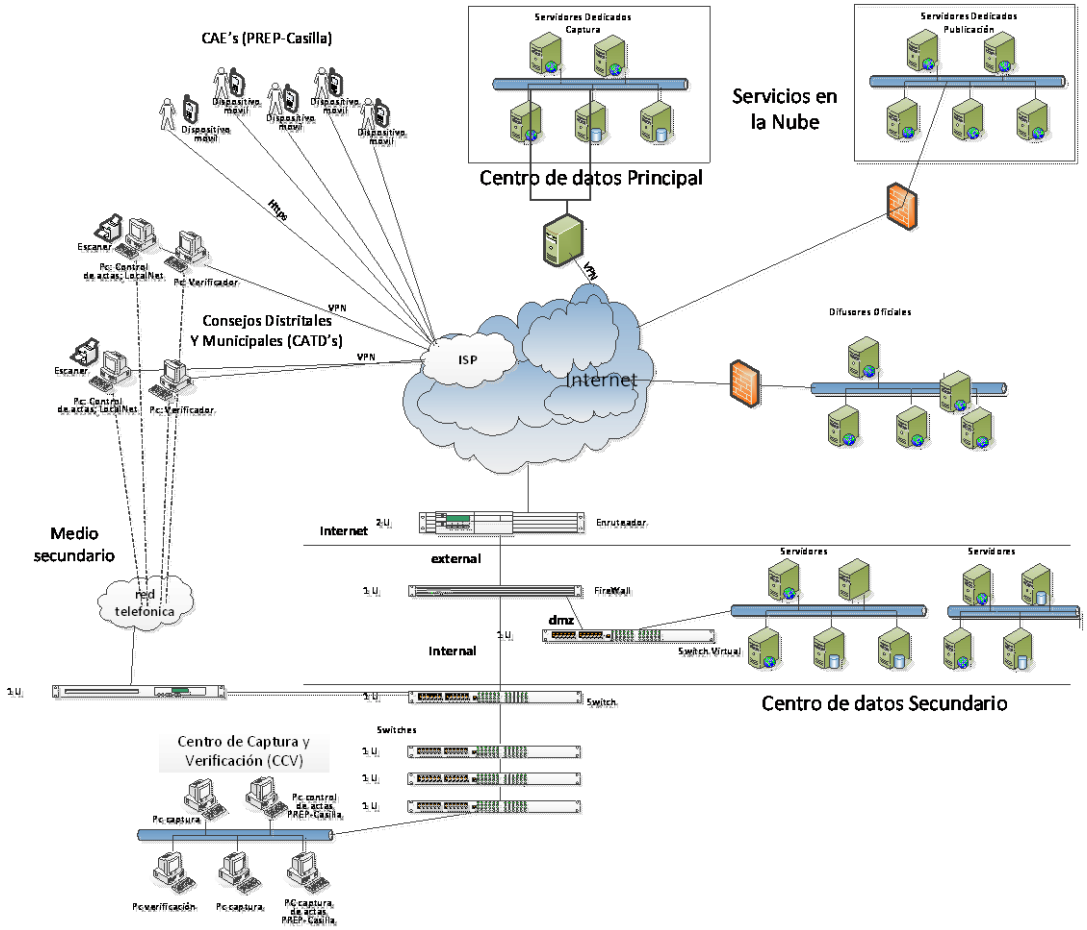

Imagen1. Diagrama con equipos involucrados en la implementación del Programa de Resultados Electorales Preliminares.

VIII.1 Políticas de seguridad para el uso de los equipos de cómputo instalados en los CATD o CCV para la implementación del PREP

Cada computadora empleada para implementar el PREP en el CATD o CCV:

- Solo tendrá instalado el software requerido para los sistemas del PREP;
- Tendrá instalado antivirus;
- Contará con contraseña de inicio de sistema;
- No se podrá instalar ningún otro software ajeno al procedimiento del proceso técnico operativo PREP;
- No se podrá instalar ningún periférico ajeno al procedimiento del proceso técnico operativo PREP;
- No se podrá insertar memoria USB ajena al procedimiento del proceso técnico operativo PREP;
- No se podrá insertar disco compacto o DVD ajenos al procedimiento del proceso técnico operativo PREP;
- No podrá ser utilizada por persona ajena al procedimiento del proceso técnico operativo PREP;
- No podrá ser conectado a la red para transferencia de datos PREP ningún equipo ajeno al procedimiento del proceso técnico operativo PREP;

Para iniciar la captura, digitalización y verificación de los resultados electorales preliminares se necesita que cada operador ingrese su clave personal de acceso evitando de esta forma que personal ajeno a esta actividad se involucre en ella.
Personal de oficinas centrales estará distribuido en los distintos CATD el día de la Jornada Electoral, personal que contará con equipo de cómputo, escáner, no-break, que en su caso, serán trasladados al Consejo Distrital o Municipal, que los requiera.

VIII.2 Políticas de seguridad para el uso de dispositivos móviles que serán empleados para la implementación del PREP-casilla.

Cada dispositivo móvil para implementar en el PREP-Casilla:

- Solo tendrá instalado el software requerido para el funcionamiento de la aplicación PREP-Casilla. No se podrá instalar ningún otro software ajeno al procedimiento del Proceso Técnico Operativo;
- Tendrá activado el bloqueo de pantalla;
- No se podrá conectar a ninguna computadora;
- No podrá ser utilizado por persona ajena al procedimiento PREP-Casilla;

Lo anterior es atendido utilizando una aplicación que es instalada en cada equipo móvil así como con el recibo donde se especifican políticas de uso del mismo.

Para iniciar la captura de la imagen del AEC se necesita que se valide el código que identifica como único al dispositivo móvil y que cada operador ingrese su usuario y contraseña, evitando de esta forma que personal ajeno a esta actividad se involucre en ella.

VIII.3 Políticas de seguridad del centro de datos

Equipo de respaldo. En el centro de datos se debe contar con equipo de cómputo que servirá de respaldo tanto para el equipo que procese la información, como para el equipo difusor.

Respaldo de información. Toda la información contenida en los servidores debe almacenarse por duplicado en dispositivos diferentes, procurando así que no exista pérdida de información.

Actualizaciones. Los equipos utilizados deben contar con sistemas operativos que reciban actualizaciones vigentes y solución antivirus actualizada. Debe existir un criterio definido para la instalación de las mismas.

Mantenimiento preventivo. La institución cuenta con objetivos estratégicos anuales para mantenimiento correctivo y preventivo de bienes informáticos como puede constatarse en los objetivos particulares 8.2.5 y 8.2.6 de las Políticas y Programas 2018.

Acceso restringido. El acceso al centro de datos, tanto físico como virtual es solo para personal autorizado. Los servidores involucrados en la implementación del PREP cumplen con los requisitos mínimos de seguridad en contraseñas. En caso de ser necesario el ingreso de un tercero deberá anotarse en bitácora de visita y personal de la DESI estará presente. Toda persona que ingresa al instituto debe portar un gafete

Monitoreo de equipos. Los equipos dentro del centro de datos (equipo de red y servidores) son monitoreados constantemente a través de una aplicación que monitorea: utilización CPU; resumen de disco duro IO; espacio en disco(s) duro; uso de Interfaz(es) de red; uso de memoria RAM y archivo de paginación; resumen de servicios; fecha y hora del sistema; tiempo en funcionamiento; logs de aplicación, hardware, key management service, seguridad, sistema, PowerShell. Además el centro de datos cuenta con equipo de monitoreo de ambiente (temperatura, humedad) que notifica de manera automática la salida de rango de algún indicador. A cargo del monitoreo tanto de la aplicación como del equipo de monitoreo de ambiente está la coordinación de infraestructura de red.

Manejo de código malicioso. El centro de datos debe contar como mínimo con equipo de seguridad en la red que además de fungir como firewall, proteja contra amenazas en la red (ataques, virus, gusanos, etc.)

VIII.4 Seguridad en la transmisión de datos

Los enlaces de telecomunicaciones son probados en su funcionamiento una y otra vez a lo largo del proceso electoral, ya que los Consejos Electorales Distritales y Municipales cuentan con sistemas de información automatizados que requieren estar enviando información, de manera similar a la que se transmitirá el día de la Jornada Electoral. Con estas medidas se hace confiable la transmisión de los resultados electorales.

En la mayoría de los CATD y CCV se utiliza un equipo (hardware) diseñado exclusivamente para efectuar tareas específicas de seguridad en la red con el que se establece la conexión vía VPN con el centro de datos principal y secundario. El equipo está configurado con políticas estrictas para el tráfico de información desde y hacia internet. Donde no es posible utilizar este equipo la VPN se genera a través de un software que se instala en los equipos donde se efectúa la captura y verificación de datos.

Los datos que se transmiten entre el centro de datos y los Consejos Electorales Distritales y Municipales lo hacen a través de una VPN. La VPN permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

La transmisión de datos entre los dispositivos móviles y el centro de datos será cifrada.

Cada CATD establece una VPN al centro de datos primario y una VPN al centro de datos secundario. Los CATD con el mayor número de casillas cuentan con servicio de internet redundante.

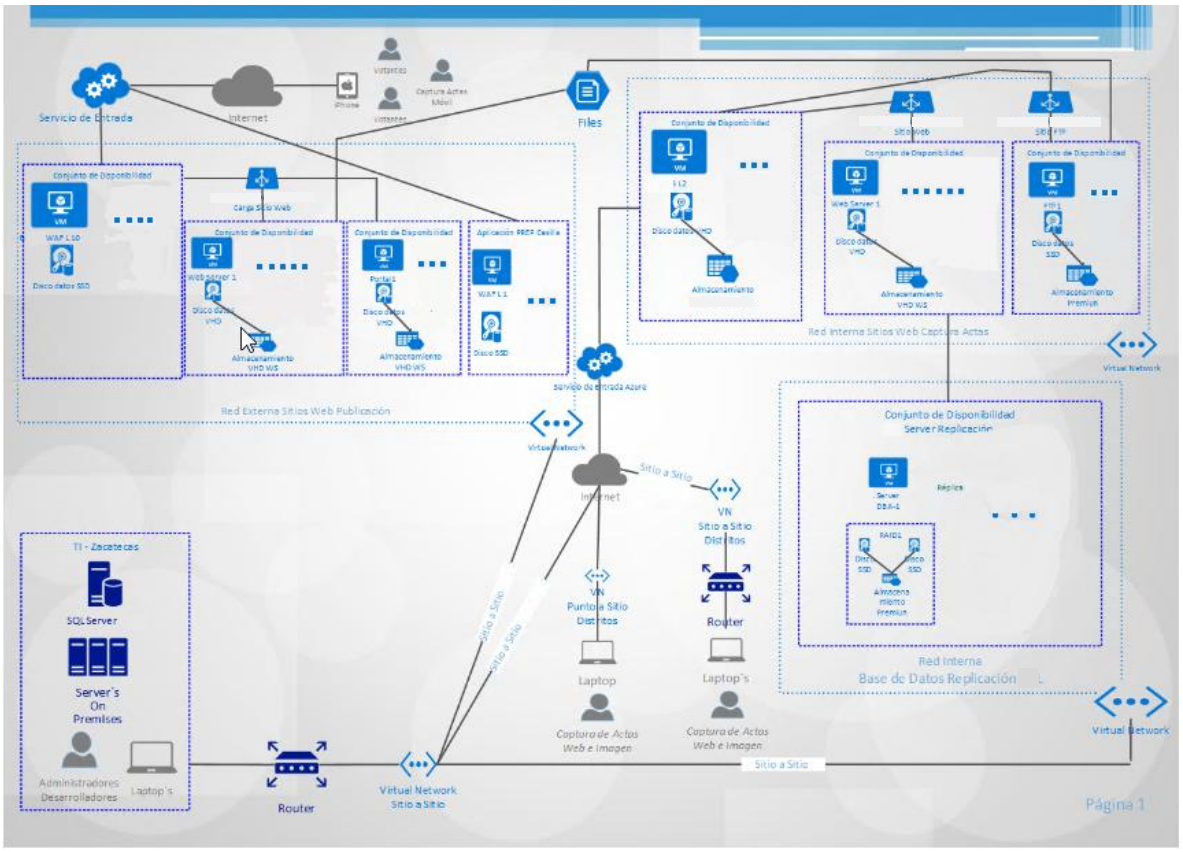

Imagen 2. Diagrama de red de comunicaciones

VIII.5 Infraestructura tecnológica

Sistema informático PREP. Se cuenta con experiencia en el desarrollo de esta solución por parte del Instituto, a pesar de esto, es necesaria la ejecución de pruebas del funcionamiento de las diferentes etapas del sistema. Es necesario el cotejo de los catálogos de la información electoral (partidos, coaliciones, candidatos independientes, secciones, casillas, etc.) para la funcionalidad del sistema.

Servidores web y de bases de datos. Para garantizar la disponibilidad del servicio, se cuenta con un centro de datos principal y uno secundario. Cada centro de datos cuenta con equipos de respaldo y de seguridad en la red. Los equipos del CATD y CCV se encuentran conectados simultáneamente al centro de datos primario como al secundario, lo que permite que puedan redirigir el tráfico de uno a otro con un cambio de direccionamiento de los equipos de captura, digitalización y verificación. Véase imagen 1.

Equipo de red. Este punto de la infraestructura es crucial, por lo que se cuenta con equipo de red de manufactura reciente y de marcas líderes en el mercado. Se encuentran actualizados y expertos en su administración dan soporte para su implementación. Se hace uso de dispositivos con detección firewall, detección de

intrusos, antivirus y con políticas de control de tráfico entre segmentos de red. El equipo de red se configura implementando segmentación VLAN con políticas de seguridad a nivel capa 2 y capa 3. La infraestructura implementada para el PREP en el sitio secundario se encuentra aislada en su propio segmento de red con sus propias políticas de acceso, lo mismo opera para el sitio primario.

Enlaces de telecomunicaciones. En el centro de datos secundario se cuenta con un servicio de carrier de Fibra óptica suministrada por Telmex.

Enlaces de internet de los CATD y CCV. En los CATD y CCV se cuenta con servicios de infinitum proporcionado por Telmex. En algunos CATD se cuenta con el servicio de internet proporcionado por otro proveedor. La comunicación entre los CATD's y los centros de datos principal y secundario viaja a través de una VPN donde la información viaja por un canal seguro.

En caso de fallo del servicio de internet, los CATD pueden llevar el proceso de captura, verificación y digitalización y hacer la transmisión de los datos capturados (excepto imágenes) vía conexión modem, y las imágenes deberán ser transmitidas en oficinas del CATD más cercano.

Personal de soporte. El Instituto cuenta con el soporte técnico especializado proporcionado por el proveedor de donde se encuentra albergado el centro de datos principal así como el soporte de personal especializado en equipo de red y de seguridad. Este personal estará presente a lo largo de la Jornada Electoral y estarán solamente para labores de monitoreo y de apoyo para restablecer el sistema en caso de alguna eventualidad.

Auditoría PREP. Tanto la infraestructura tecnológica como los sistemas informáticos son sometidos a una auditoría enfocada principalmente: pruebas funcionales de caja negra al sistema; validación del sistema informático del PREP y sus bases de datos; análisis de vulnerabilidades a la infraestructura tecnológica; pruebas de denegación de servicio a sitios web del PREP y al sitio principal del Instituto Electoral del Estado de Zacatecas.

VIII.6 Seguridad en la captura

Se establecen controles para brindar un alto grado de seguridad al proceso de captura de las Actas PREP, entre los que se distinguen los siguientes:

Para el ingreso al sistema de captura, digitalización y verificación es necesario, en primera instancia, contar con el usuario y contraseña que permite inicializar el equipo de cómputo.

Con el equipo de cómputo operando en los CATD o CCV, y una vez ingresado al sistema, el cual requiere de otro usuario y contraseña, dentro del proceso de captura se cuenta con una doble captura de los datos, reduciendo así la

posibilidad de errores humanos. Aunado a esto, después de la doble captura se ingresa una contraseña más garantizando que los datos a registrar provienen de un usuario autorizado. Adicionalmente, un verificador deberá revisar y cotejar que los datos capturados en el sistema informático coincidan con la información plasmada en el AEC, a través de la imagen digitalizada. Los usuarios y contraseñas son reemplazados antes del día de la jornada y la contraseña final de captura (captura, verificación) es entregada a través de un protocolo formal el día de la Jornada Electoral por el Presidente del Consejo Distrital o Municipal.

La autenticidad e integridad de cada una de las transacciones que sean enviadas al centro de datos primario están protegidas dado que la conexión al centro de datos se realiza dentro de una VPN establecida entre el CATD o CCV y el centro de datos principal.

Para el ingreso a la aplicación de captura de imágenes de las AEC desde casilla es necesario en primera instancia acceder al dispositivo móvil ingresando el PIN que desbloquee la pantalla, que el dispositivo móvil cuente con un identificador único válido, un usuario y contraseña que permita inicializar la aplicación.

Con el dispositivo móvil operando y una vez ingresado a la aplicación el operador deberá seleccionar, de una lista de casillas correspondientes a su área de responsabilidad, la sección, casilla y tipo de elección de la imagen del AEC a capturar.

VIII.7 Seguridad en la publicación

Para garantizar la alta disponibilidad del PREP para su consulta a través de internet, se implantó una arquitectura paralela de servidores, interconectados entre sí. Lo anterior sin contar la difusión que se llevará a cabo a través de los difusores oficiales que apoyarán con la publicación de la información a través de sus correspondientes portales de internet. El proveedor de servicios en la nube cuenta con las siguientes certificaciones:

▪ Microsoft Gold Cloud Platform ▪ Microsoft Gold AER ▪ Microsoft Silver Cloud Productivity ▪ Microsoft Silver Application Development ▪ Microsoft Silver Datacenter ▪ Microsoft Silver Hosting ▪ Microsoft CSP Tier 1	▪ Distribuidor Certificado Hewlett Packard Enterprise ▪ Premier Cisco Partner ▪ Meraki Partner ▪ VMWare Professional Partner ▪ Distribuidor Certificado Bitam ▪ Distribuidor Certificado Genexus

El nivel de servicio o SLA que ofrece es de 99.95% y el proveedor es quien proporciona los recursos necesarios para obtener esta alta disponibilidad en los recursos, véase https://azure.microsoft.com/en-us/support/legal/sla/virtual-machines/v1_8/

.

VIII.8 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 como: condiciones de humedad, aire acondicionado, sensores de incendio, alimentación eléctrica, etc.
Se plantean como políticas de seguridad física y ambiental las siguientes:

- Acceso restringido en el centro de datos principal (Como se menciona en las políticas de seguridad para el centro de datos).
- Cámara IP instalada en el centro de datos.
- Sistema de control ambiental (Como se menciona en las políticas de seguridad para el centro de datos).
- Seguridad perimetral en el centro de datos así como en cada uno de los CATD.
- Registro de personal que accede al centro de datos (Como se menciona en las políticas de seguridad para el centro de datos).
- Solo personal autorizado tanto en centro de datos como en los CATD.
- Sistema de detección de incendios y extintor para incendios eléctricos en centro de datos.
- Suministros de energía redundantes en equipos involucrados en alguno de los procesos PREP.
- Revisiones y mantenimiento de los servidores de aplicaciones y de base de datos.

VIII.9 Seguridad de la energía eléctrica

Planta de energía de emergencia en centro de datos. Se cuenta con una planta de energía eléctrica de emergencia con la capacidad suficiente para soportar la carga de energía de todo el edificio del Instituto, no solo los servidores, computadoras y demás equipos de telecomunicaciones. Además el centro de datos cuenta con equipo de respaldo de energía en caso de falla y para operar en tanto entra en funcionamiento la planta de energía externa.

Planta de energía de emergencia en cada uno de los CATD. Se cuenta con una planta de energía eléctrica de emergencia en los CATD. Además los equipos de cómputo cuentan con equipo de respaldo de energía en caso de falla, para operar en tanto entra en funcionamiento la planta de energía externa.

VIII.10 Plan de Continuidad

Véase Plan de Continuidad del Programa de Resultados Electorales Preliminares para la elección de Diputados y Ayuntamientos en el Proceso Electoral 2017-2018.