PREP 2024 • VER

OPLE Veracruz
ORGANISMO PÚBLICO LOCAL ELECTORAL

Plan
Versión 1.2

Plan de seguridad PREP 2024

OPLE Veracruz

Marzo 2024

Informática Electoral

Contenido

Tabla de Contenido

Tabla de Ilustración

Glosario

Acta PREP: Acta de Escrutinio y Cómputo destinada para la operación PREP.

AES: Estándar de Encriptación Avanzada (Advanced Encryption Standard).

AWS: Servicios Web de Amazon (Amazon Web Services).

CATD: Centro de Acopio y Transmisión de Datos.

Cableado de red: Es la infraestructura necesaria para conectar equipos informáticos a la red por medio de cables de cobre o fibra óptica.

Categoría de cable: Se refiere a las características de desempeño que tiene un cableado de red. Iniciando con la categoría 5e soporta velocidades de transmisión de datos de hasta 1000 Mbps. En mayor sea la categoría mejor será el desempeño mostrado. Así un cable categoría 6 tiene mejor desempeño que la categoría 5e.

CCTV: Circuito Cerrado de Televisión

CCV: Centro de Captura y Verificación.

COPREP: Centro de Operaciones del Programa de Resultados Electorales Preliminares.

CVPREP: Módulo de Captura y Verificación PREP.

DDoS: Ataque Distribuido de Denegación de Servicio.

DNS Rebind: Técnica de ataque informático que explota la forma en que los navegadores web implementan la política de mismo origen (Same-Origin Policy) para acceder a recursos en diferentes dominios.

Firewall: Programas de software o dispositivos de hardware que filtran y examinan la información que viene a través de su conexión a Internet.

GBPS: Gigabits por segundo.

HASH: Es una función matemática que toma una entrada y produce, de manera prácticamente univoca, una cadena de caracteres de longitud fija.

HTTPS: Protocolo de Transferencia de Hipertexto Seguro.

IDS: Sistema de Detección de Intrusiones (Intrusion Detection System).

IPS: Sistema de Prevención de Intrusiones (Intrusion Prevention System).

ISP: Proveedor de Servicios de Internet (Internet Service Provider).

ISO: Organización Internacional de Estandarización (International Organization for Standardization).

IBM: Corporación Internacional de Máquinas Electrónicas (International Business Machines Corporation).

ISO 27001: Estándar internacional para la gestión de la seguridad de la información, que establece requisitos y mejores prácticas para la implementación de un sistema de gestión de seguridad de la información.

MCAD: Módulo de Revisión de Imágenes Digitales e Identificación de Acta de Escrutinio y Cómputo.

OPLE Veracruz: Organismo Público Local Electoral del Estado de Veracruz.

PREP: Programa de Resultados Electorales Preliminares.

Restricciones L: Restricciones de licencia.

Root: Se refiere al acceso de nivel más alto en un sistema informático o dispositivo, también conocido como “Superusuario”

SIPREP: Sistema de Información del Programa de Resultados Electorales Preliminares.

TBPS: Terabits por segundo.

VLAN: Una VLAN, acrónimo de virtual LAN (Red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física, aun superadas geográficamente. Brinda seguridad a un grupo de trabajo aislado los dominios de broadcast.

VPN: Una Red Privada Virtual (RPV), en inglés: Virtual Private Network (VPN), es una tecnología de red de computadoras que crea un túnel seguro en internet (utilizando técnicas de autentificación y de autentificación y encriptación) y permite la conexión de redes que se encuentran en diferentes zonas geográficas.

1 Introducción

El presente documento fue elaborado con la finalidad de presentar la metodología y los mecanismos de seguridad de la información destinados a ser implementados en la solución PREP durante el Proceso Electoral Local Ordinario 2023-2024 del estado de Veracruz.

Estos mecanismos tienen como objetivo principal salvaguardar la integridad, disponibilidad y confidencialidad de la información, fundamentándose en las mejores prácticas y los estándares más rigurosos de acuerdo con las directrices de organismos internacionales, actuando en conformidad con la norma ISO 27001.

2 Plan de seguridad

La seguridad con la cual se maneja la información es uno de los puntos más importantes, por ello Informática Electoral propone el siguiente plan de fortalecimiento de seguridad para garantizar el flujo e integridad de la información, Este plan se compone de dos esquemas: uno para respaldar el proceso de preparación a la elección y otro, con una mayor robustez, para soportar el día de la jornada electoral (la operación del PREP).

2.1 Arquitectura de seguridad

Los sistemas informáticos PREP serán habilitados en un sistema de nube híbrida, combinando una nube privada, alojada dentro del CCV principal y dotada con seguridad perimetral a través de firewalls, y un servicio de nube pública con mecanismos y tecnologías de seguridad perimetral.

La arquitectura de seguridad contempla varios niveles de protección:

- A nivel de comunicaciones entre los diferentes puntos de presencia
- A nivel de publicación de la información

Para garantizar la comunicación entre los diferentes puntos de presencia se utilizarán túneles VPN con encriptación de datos AES de 256 bits para la comunicación de sitios remotos. Los servidores utilizaran balanceadores de carga para que distribuyan las peticiones de los usuarios y evitar su saturación. Dentro de los centros de datos, se utilizarán VLAN, y firewalls para proteger la red interna, además de Sistemas de Prevención de Intrusos / Intrusion Prevention Systems (IPS) y Sistemas de elección de Intrusos / Intrusion Detection System (IDS), para evitar accesos no autorizados.

Para garantizar la publicación de información del sitio web público, se dispondrá de protección de ataques DDoS, capaz de mitigar ataques de denegación de servicio de más de 200Tbps. También se implementará un firewall de aplicaciones web (WAF por sus siglas en inglés) y una red de entrega de contenidos (CDN, por sus siglas en inglés) con más de 200 puntos de presencia a nivel mundial y con capacidad de entregar 50 Gbps de sitio web. Este servicio mitigará los posibles ataques y enviará las

peticiones legítimas a un balanceador de carga redundante con capacidad de 250,000 conexiones únicas.

El balanceador de carga redundante enviará las peticiones a las instancias de servidores web necesarios para entregar los contenidos. Dependiendo del número de visitante se considera necesario que el balanceador despliegue de 2 a 10 instancias para atender la demanda.

2.2 Estructura del modelo de seguridad

En Informática Electoral, proponemos una estructura avanzada de modelo de seguridad que asegura la operatividad ininterrumpida y la integridad de los sistemas. Esta estructura se fundamenta en la utilización dual de centros de datos: el Centro de Datos Primario (CD1) y el Centro de Datos de Contingencia Remoto (CD2). El CD1 sirve como el núcleo inicial para el almacenamiento de datos, mientras que el CD2 actúa como un respaldo en tiempo real y esencial para la continuidad del negocio, garantizando así la disponibilidad y la resiliencia del sistema frente a incidentes imprevistos.

La replicación de datos entre estos centros se configura para ser inmediata para información crítica, incluyendo bases de datos y Actas PREP digitalizadas, y se realiza con un diferencial de 60 segundos para datos considerados de menor criticidad, como son los contenidos estáticos de servidores de publicación y servicios secundarios. Este enfoque garantiza una disponibilidad continua de los servicios principales, incluidos los servidores de almacenamiento y captura de Actas PREP, los servidores de bases de datos, y los servidores dedicados a la difusión pública de resultados.

Selección de Proveedores de Nube Pública y Cumplimiento de Estándares

Informática Electoral se compromete con la seguridad y la eficacia de las infraestructuras tecnológicas implementadas. Es por ello por lo que hemos seleccionado AWS e IBM Cloud como nuestros principales proveedores de servicios en la nube, basándonos en su amplia trayectoria y su probado cumplimiento con estándares de seguridad de información de nivel mundial. Estas plataformas han sido rigurosamente evaluadas y seleccionadas por cumplir y superar las expectativas en cuanto a:

Estándares Internacionales de Seguridad: AWS e IBM Cloud están certificados bajo las normativas ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO 27017, e ISO 27018, lo que asegura la adopción de un Sistema de Gestión de Seguridad de la Información (SGSI) efectivo, junto con controles de seguridad especializados para entornos de nube.

Evaluaciones de Seguridad por Terceros: Ambos proveedores disponen de informes SOC tipo 2, confirmando la seguridad, la disponibilidad, y la confidencialidad de sus servicios, verificados por auditorías independientes.

Adhesión y Conformidad con CSA: Registrados en la Cloud Security Alliance (CSA) y cumpliendo con la autoevaluación voluntaria del Security, Trust & Assurance Registry (STAR) de CSA, AWS e IBM Cloud demuestran su compromiso con las mejores prácticas de seguridad en la nube.

Adopción de CIS Security Benchmarks: La implementación de programas basados en los CIS Security Benchmarks por parte de estos proveedores facilita a Informática Electoral a la evaluación y mejora continua de la seguridad, conforme a las mejores prácticas industriales.

La inclusión de AWS e IBM Cloud en nuestra arquitectura de seguridad no solo refleja nuestro compromiso con la excelencia operacional y la seguridad de los datos, sino que también asegura el cumplimiento con las directrices y recomendaciones establecidas en el Plan de Seguridad del INE. Informática Electoral mantiene un enfoque proactivo hacia la innovación tecnológica y la adopción de estándares internacionales de seguridad, con el objetivo de proporcionar una infraestructura electoral robusta, confiable y segura.

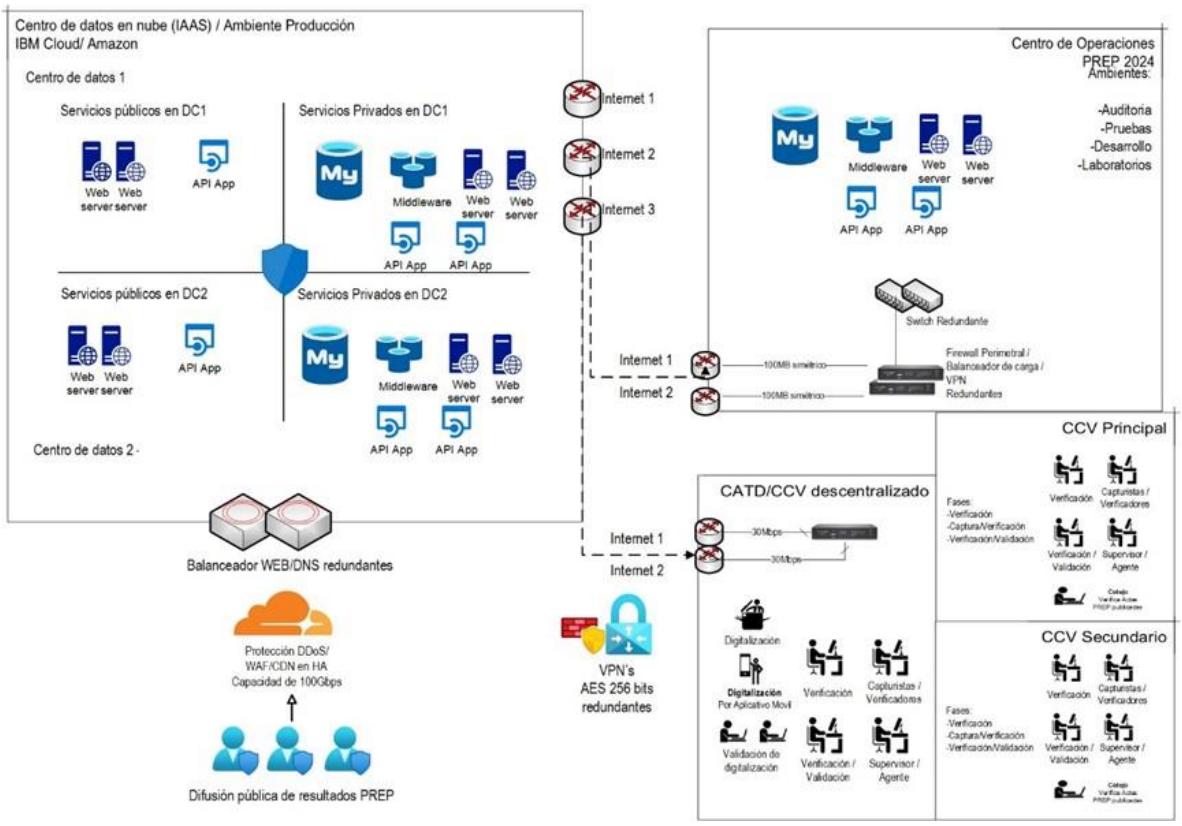


Ilustración 1. Diagrama de interconexión y seguridad de red

2.3 Estrategia de gestión de riesgo

Para mitigar los riesgos relacionados con amenazas identificadas y posibles ataques a los centros de datos y páginas web oficiales, se propondrá una estrategia que incluya:

1. Realización de un análisis detallado de cada contingencia, evaluando su nivel y probabilidad de impacto.
2. Desarrollo de grupos de respuesta con medidas específicas para abordar cada amenaza identificada de manera inmediata.

Estrategias que se pueden consultar en el formato: ***PLAN CONTINUIDAD.***

2.4 Análisis de riesgos de los activos

La información detallada sobre el análisis de riesgo sobre los activos de información, servicios, personas, intangibles está disponible en el documento ***PLAN CONTINUIDAD,*** específicamente en las tablas 7.4, 7.5,7.6, 7.7 en las cuales se puede observar el análisis de riesgo de cada uno de los activos al igual que las acciones para mitigar los riesgos identificados.

2.5 Mecanismo de seguridad

Para asegurar que existan las adecuadas medidas de seguridad para la protección de la información y de los sistemas, se implementaran los siguientes controles.

- Control de usuarios y contraseñas con privilegios de operación
- Comunicación cifrada de información
- Implementación de red segura y estructura de servidores
- Mecanismos de redundancia de información y comunicación
- Bitácora de operaciones
- Protección de sitio web público
- Listado de verificación de seguridad
- Seguridad de los datos

2.5.1 Mecanismos de Seguridad de acceso físico

- Control de Acceso Físico: Implementación de sistemas de acceso físico, como tarjetas de acceso, guardias de seguridad, para garantizar que solo las personas autorizadas puedan ingresar a las instalaciones.
- Vigilancia y Monitoreo: Instalación de cámaras de seguridad y sistemas de monitoreo para supervisar las áreas críticas y detectar cualquier actividad sospechosa.
- Políticas de Seguridad Física: Desarrollo y aplicación de políticas y procedimientos específicos para la seguridad física, incluyendo la identificación de puntos de acceso, la asignación de responsabilidades y la respuesta a incidentes.

2.5.2 Mecanismos de Monitoreo de servicios

- Sistema de Monitoreo de Servicios: Implementación de un sistema de monitoreo continuo de los servicios críticos del sistema, como servidores de bases de datos, servidores de aplicaciones, servicios de red, etc. Este sistema debería supervisar el rendimiento, la disponibilidad y la integridad de los servicios, y alertar al personal de operaciones en caso de cualquier anomalía o interrupción.
- Capacitación y Concienciación del Personal: Capacitar al personal de seguridad y a los operadores del sistema en la identificación y respuesta a eventos de seguridad.
- Gestor de dispositivos móviles: Se utilizará un gestor de dispositivos móviles para mejorar la seguridad y monitorear los equipos móviles
- The Dude: Se utilizarán programas para monitorear, mapear y gestionar remotamente la red, como el caso del programa The Dude

2.5.3 Control de usuarios y contraseñas con privilegios de operación

Dado que el PREP es un sistema en línea, es necesario que disponga de un mecanismo de acceso, por lo tanto, se implementará un estricto control y generación de las cuentas de usuario correspondientes. Como segundo nivel de seguridad en este rubro, es preciso señalar que el PREP contemplará diversos niveles de privilegios de operación dependiendo de los roles en las cuentas de usuario. Por ejemplo, un usuario encargado de digitalizar e identificar las Actas PREP en el CATD del Distrito 5 no podrá digitalizar e identificar Actas PREP e información del CATD del Distrito 4. Asimismo, los usuarios de tipo “consulta”, no podrán capturar información, tal como sugiere su denominación.

Es importante destacar que todos los equipos de cómputo utilizados en el PREP estarán completamente actualizados en cuanto al sistema operativo, hardware y antivirus. Asimismo se cuenta con procedimientos establecidos y probados para la administración y configuración de los dispositivos de comunicaciones, servidores y base de datos para evitar vulnerabilidades en durante su operación, siendo señalados en el plan de habilitación y desinstalación, así como en el plan de capacitación y entrenamiento.

Para garantizar la seguridad de las contraseñas a utilizar, se establecerá una longitud mínima y un nivel de complejidad adecuado. Estas contraseñas serán renovadas previo al inicio de cada ejercicio, simulacro y jornada electoral.

Además, para reforzar la seguridad de los equipos de cómputo a utilizarse en el PREP, se inhabilitan los puertos USB de cada uno de los dispositivos, de la misma manera se inhabilitara e impondrán restricciones en las tarjetas de red inalámbrica (Wi-Fi) y Bluetooth, y bandejas lectoras de CD/DVD.

Este procedimiento evita filtración de información y protege al equipo contra la introducción de virus informáticos.

Los usuarios se generarán bajo la siguiente nomenclatura:

[SISTEMA]_[CENTROID]_[NUMERO_USUARIO]

Ejemplo: Cvprep_40_01

Las contraseñas asociadas a estas cuentas se generarán desde un sistema central, siguiendo las siguientes reglas:

- 8 caracteres alfanuméricos (Números, mayúsculas, minúsculas y caracteres especiales).
- Se generarán contraseñas únicas de manera aleatoria.
- Se realizará una asignación de contraseñas de manera periódica
- Las contraseñas se resguardarán de manera segura en las oficinas de Informática Electoral.
- Estará estrictamente prohibido registrar contraseñas en cualquier lugar del espacio de trabajo.

2.5.4 Comunicación cifrada de información

Para fortalecer los mecanismos de envío de la información a través de Internet, se implementarán en firewalls un mecanismo de encriptación de 256 bits. Esto establecerá canales seguros entre los CATD's, CCV's y COPREP mismo que tiene un área determinada dentro del CCV Secundario, además la comunicación a los servidores del sistema será a través de protocolos seguros en específico HTTPS, aunado a esto una doble autenticación de acceso. Dicho protocolo (HTTPS) es el mecanismo estándar a nivel internacional en materia de transmisión de datos sensibles en sistemas de comercio electrónico y servicios bancarios en línea.

2.5.5 Implementación de red segura y estructura de servidores

A la par del uso de protocolos cifrados para el envío de la información, se establecerá una red privada virtual (VPN) con nivel de encriptación de 256 bits entre los equipos de cómputo instalados en los CATD's y en oficinas centrales del OPLE Veracruz con los servidores que alojen los sistemas del PREP. Cabe señalar que solamente los equipos que estén dados de alta en dicha red privada podrán acceder al sistema, incrementando con ello su nivel de seguridad.

Los firewalls instalados en CATD's / CCV's y el Centro de Operación, tendrán reglas que permitirán el acceso únicamente a los equipos de cómputo necesarios y estrictamente a los servicios que se requieren.

Esta red segura contempla el uso de sistemas de protección contra ataques de diversos tipos, tales como: Ataques "Hombre en el Medio" (MITM) que permiten interceptar el tráfico entre un servidor y un equipo de cómputo, ataques de "DNS rebind" que permiten convertir un equipo en un proxy de red, entre otros.

2.5.6 Mecanismos de redundancia de información y comunicación

Para el almacenamiento de la información proveniente de los CATD's, se implementará un sistema de redundancia utilizando al menos dos servidores locales que funcionarán en modo espejo o

equivalente, que permite respaldar la información de un servidor a otro en tiempo real, por si alguno de los dos sufriera algún daño, la información seguirá disponible.

En caso de existir cortes de señal de Internet en algún componente de la red privada, cada CATD, CCV y Centro de Operaciones deberá contar con un enlace alterno, para mantener comunicación con los servidores del sistema.

Ejemplos de servicio de Internet en Centro de Operaciones:

- ISP1 como principal, con ancho de banda suficiente para sostener la operación fluida y al menos un 50% de excedente.
- ISP2 como secundario, con ancho de banda suficiente para sostener la operación fluida y al menos un 50% de excedente.

2.5.7 Bitácora de operaciones

El sistema de captura con múltiples usuarios cuenta con un control o bitácora de operaciones realizadas en el sistema, que incluye desde fecha y hora de ingresos y salidas del sistema hasta registro de operaciones de captura y consulta de todos los usuarios que tengan contraseña válida para utilización del sistema.

2.5.8 Protección de sitio web público

Para la publicación del sitio web público, se contará con un servicio de protección de ataques DDoS con capacidad de 100 Gbps, un firewall de aplicaciones web (WAF por sus siglas en inglés) y una red de entrega de contenidos (CDN por sus siglas en inglés) con más de 200 puntos de presencia a nivel mundial y capacidad de entregar al menos 50 Gbps de sitio web.

Este servicio mitigará los posibles ataques y enviará las peticiones legítimas a un balanceador de carga redundante con capacidad de 250,000 conexiones únicas.

El balanceador de carga redundante enviará las peticiones a los servidores web necesarios para entregar los contenidos, pudiendo ser desde 2 hasta 10, dependiendo del probable número de visitantes que espere el sitio web público, en este caso en particular, se definió el uso de 8 servidores.

2.5.9 Listado de verificación de seguridad

El listado de verificación de seguridad es una herramienta utilizada para asegurar que se cumplan todos los pasos necesarios establecidos para garantizar la seguridad en las actividades y procesos. Consiste en una serie de requerimientos que deben ser revisados y abastecidos con el fin de evitar posibles fallos o identificar áreas de mejora en el sistema de seguridad.

Con el fin de fortalecer la gestión y seguimiento de las actividades e infraestructura de los componentes tecnológicos que se utilizarán en los simulacros y el día de la jornada electoral.

2.5.10 Seguridad de los datos

Para realizar el proceso PREP Informática Electoral suministrará y hará la configuración y pruebas necesarias de los siguientes equipos informáticos en cada CATD y en su caso CCV:

- Equipo para conectividad y seguridad de red: Firewall perimetral, realizará el balanceo de ancho de banda de los internet, habilitación de la red privada virtual.
- Equipo conmutador de red: Se interconectarán los equipos de cómputo y tecnológicos para crear una red LAN.
- Teléfono IP: Equipo configurado con una línea y extensión interna, la cual se comunicará entre CATD's y COPREP mediante VPN.
- Cableado de red: Todos los equipos de cómputo se comunicarán mediante cableado Ethernet categoría 6e con una velocidad de 10/100 Mbps como mínimo en los CATD.
- Y, cableado Ethernet categoría 6 en el caso de los CCV.

2.6 Seguridad física en CATD y CCV

Se implementarán las siguientes medidas en todos los inmuebles de manera prioritaria y sin excepción:

- Contar con excelentes condiciones de construcción para evitar posibles filtraciones de aire y agua que dañen el equipo tecnológico. También debe de contar con facilidad para la instalación de servicios externos, tales como telefonía e internet.
- Extintores de CO2, que no dañen el equipo de cómputo al ser usados, distribuidos 1 cada 300 metros cuadrados de acuerdo con lo indicado en la NOM-002-STPS-2010.
- Área libre de ventanas, en caso de existir estas deben de contar con protecciones y cerrojo.
- Es deseable que solo se cuente con una puerta de acceso, la cual debe de contar con cerrojo y acceso biométrico para el control de acceso al personal.
- En el caso de las instalaciones donde vayan a trabajar más de 50 personas, será recomendable que el recinto cuente con salida de emergencia.
- Conexiones eléctricas suficientes para la conexión de los equipos informáticos: En el espacio designado como CATD y/o CCV debe haber al menos una conexión de corriente eléctrica regulada y aterrizada a tierra, la cual se conectará al UPS que proporcione Informática Electoral.
- Aire acondicionado: Con capacidad de abastecimiento para toda el área del CCV.
- Las comunicaciones sobre información sensible no deben llevarse a cabo en lugares donde puedan ser escuchadas, Información que pueda llevar a la identificación de individuos deberá ser evitada en las conversaciones.
- La comunicación oral de información sensible debe hacerse en áreas seguras.
- Documentos sensibles no deben ser dejados sobre impresoras, copiadoras, escritorios, etcétera.
- Documentos sensibles no deben dejarse a la vista de posibles visitantes externos.

- Si es necesario dejar documentos sensibles en áreas donde puede haber visitantes, deben colocarse con el frente hacia abajo.
- Documentos sensibles que ya no son necesarios deben destruirse inmediatamente, o colocados en contenedores apropiados para su posterior destrucción.
- Conversaciones telefónicas sobre temas sensibles deben llevarse a cabo de manera discreta.
- Cuando se trate un tema relativo a una persona en particular, confirmar de quién se está hablando antes de hacerlo.
- Si la persona a quien se quiere localizar no se encuentra únicamente dejar el nombre y teléfono a donde deberá llamar cuando esté disponible.
- Mantener bajo el volumen del altavoz.
- Si un dispositivo móvil es robado o extraviado debe ser reportado inmediatamente.

2.7 Seguridad de personal

2.7.1 Identificaciones y detección de intrusos

Se implementará una estrategia para asegurar que el acceso a los CATD y CCV's sea restringido exclusivamente a el personal autorizado por Informática Electoral y el OPLE Veracruz. Se mantendrá un registro detallado de todos los accesos.

Para reforzar la seguridad en los centros, se requerirá que todo el personal presente en dichas instalaciones porte su identificación oficial, la cual tiene en su diseño: en la parte frontal, el logo de Informática Electoral, fotografía del portador, nombre y puesto; y en la parte trasera de la identificación, la dirección de Informática Electoral, código QR, firma de autorización, clave de elector, tipo de sangre, correo, vigencia de identificación, logo del OPLE Veracruz y logo de IE.

Diseño parte frontal	Diseño parte trasera
	

Tabla 1. Diseño de gafetes

2.7.2 Chalecos

Todo el personal deberá portar chalecos oficiales que lo identifiquen como miembro del personal contratado, las cuales deberán tener los colores establecidos por Informática Electoral y el OPLE Veracruz. Los colores serán establecidos de acuerdo con el puesto que funja.

Diseño frontal	Diseño trasero
	

Tabla 2. Diseño chaleco para coordinador CATD/CCV

Diseño frontal	Diseño trasero
	

Tabla 3. Diseño chaleco para Capturista / Verificador

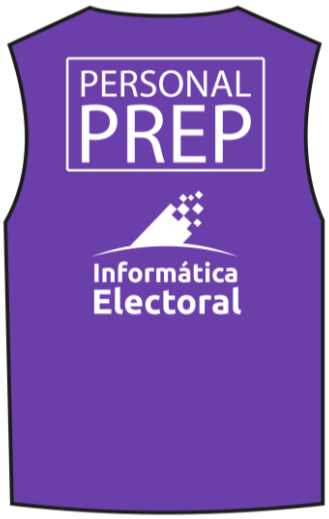
Diseño frontal	Diseño trasero
	

Tabla 4. Diseño chaleco para digitalizador

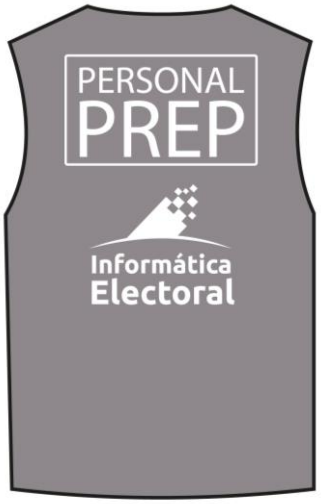
Diseño frontal	Diseño trasero
	

Tabla 5. Diseño chaleco para acopiador

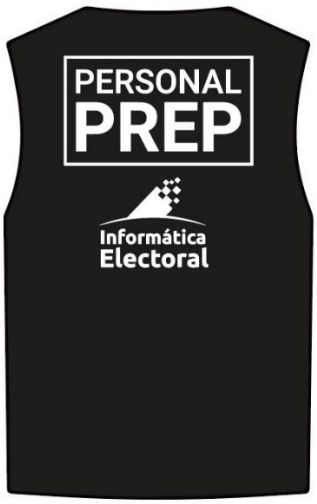
Diseño frontal	Diseño trasero
	

Tabla 6. Diseño chaleco para personal del COPREP

Monitoreo por video CCTV en los CATD y CCV, tanto a las imágenes en tiempo real, como a las grabaciones.

No se permitirá el uso de dispositivos móviles de comunicación o fotográficos personales al interior de las instalaciones, para esto se instalarán 1 línea de Voz IP a las Oficinas de Coordinación.

2.7.3 Seguridad en el acceso a la aplicación móvil

La seguridad en el acceso a aplicación móvil tiene contemplados los siguientes puntos:

- Utilización de tokens: Se empleará un token con una expiración de 2 horas el cual sólo podrá ser utilizado por el usuario al que sea asignado al inicio de la jornada y puede ser configurable con respecto a lineamientos PREP.

La seguridad en celulares:

- Los celulares no deben tener permisos de administración (específicamente para PREP Casilla y CATD Celular).
- Las digitalizaciones se guardarán en formato .jpg y esta se almacena en un espacio reservado con acceso único para la aplicación, haciendo que el uso de cualquier otra aplicación de galería no pueda acceder a las digitalizaciones.
- La información de las digitalizaciones se encriptará utilizando el algoritmo RSA y posteriormente se obtendrá el HASH de la información encriptada utilizando el algoritmo SHA-

256 el cual se genera al digitalizar el acta PREP desde el dispositivo móvil, al enviarla a MCAD para su identificación se genera otro código el cual se compara con el primero que se generó, si éstos son iguales se envía, al llegar al siguiente MCAD para su foliación se genera un 3er HASH que se compara con los primeros, este proceso se realiza para validar que la digitalización no haya sido modificada.

- Restricciones en los celulares: Se implementarán restricciones L para evitar que los usuarios puedan desactivar el servicio de Geolocalización.
- El uso de geolocalización permite monitorear si el usuario se mueve de la zona en la que se encuentra la casilla donde se le ha asignado, si este se encuentra fuera de la zona asignada la aplicación no permite captura de Actas PREP.
- Consideraciones en el uso de equipos móviles:

    - Al personal operativo se le asignará un usuario y contraseña, el cual al iniciar sesión se relacionará con el IMEI del celular y generará un token que no permitirá que el usuario inicie sesión en otro celular.
    - Al iniciar la jornada la aplicación utilizará la localización para hacer comparación con la localización de la casilla y permitir el uso de la misma si se encuentra dentro de la zona establecida en la casilla.
    - El envío de imágenes será por medio del uso de datos / internet, si no se cuenta con datos la aplicación almacenará una cola de imágenes para que al llegar a una zona con acceso a internet termine el envío de imágenes.
    - En caso de que el celular no tenga acceso a internet y por consecuente a la localización, no podrá iniciar sesión hasta que tenga conectividad.

3 Plan de continuidad

Para realizar una mejor identificación de los riesgos en cada etapa o fase del proceso, revisaremos cada fase del proceso logístico. Esto se explica a detalle en el documento ***PLAN DE CONTINUIDAD.***