Instituto Electoral y de Participación
Ciudadana del Estado de Guerrero

Plan
Versión 1.0

Plan de seguridad PREP 2024

IEPC Guerrero

Marzo 2024

Contenido

0 Prefacio 4
1 Introducción 4
2 Plan de seguridad 4
2.1 Arquitectura de seguridad 5
2.2 Estructura del modelo de seguridad 5
2.3 Estrategia de gestión de riesgo 6
3 Análisis de Riesgos 6
3.1 Niveles de contingencia 7
3.2 Probabilidad de ocurrencia 7
3.3 Evaluación de riesgo 8
3.4 Hardware 8
3.5 Software 9
3.6 Recursos humanos 9
3.7 Sitios o ubicaciones de trabajo 10
3.8 Proceso 10
3.9 Mecanismo de seguridad 10
3.9.1 Control de usuarios y contraseñas con privilegios de operación 10
3.9.2 Comunicación cifrada de información 12
3.9.3 Implementación de red segura y estructura de servidores 12
3.9.4 Mecanismos de redundancia de información y comunicación 13
3.9.5 Bitácora de operaciones 13
3.9.6 Protección de sitio web público 13
3.9.7 Listado de verificación de seguridad 14
3.9.8 Seguridad de los datos 14
3.10 Seguridad física en CATD y CCV 14
3.11 Seguridad de personal 15
3.11.1 Identificaciones y detección de intrusos 15
3.11.2 Seguridad en el acceso a la aplicación móvil 16
4 Plan de concientización 17
4.1 Introducción 17
4.2 Objetivo 17
4.3 Alcance 18
4.4 Situación actual 18
4.5 Materiales de capacitación 19
4.6 Plan de trabajo 20
4.7 Modelo de capacitación 21
4.8 Cronograma de actividades 21
4.9 Reporte de situación final 21

Glosario

CATD: Centro de Acopio y Transmisión de Datos.
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.
HASH: Es una función matemática que toma una entrada y produce una cadena de caracteres de longitud fija.
HTTPS: Protocolo de Transferencia de Hipertexto Seguro.
IEPC Guerrero: Instituto Electoral y de Participación Ciudadana del Estado de Guerrero.
IDS: Sistema de Detección de Intrusiones.
IPS: Sistema de Prevención de Intrusiones.
MCAD: Módulo de Revisión de Imágenes Digitales e Identificación de Acta de Escrutinio y Cómputo.
OPL: Organismo Público Local.
PREP: Programa de Resultados Electorales Preliminares.
SIPREP: Sistema de Información del Programa de Resultados Electorales Preliminares.
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. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.
VPN: Una Red Privada Virtual (RPV), en inglés: Virtual Private Network (VPN), es una tecnología de red de computadoras que permite una extensión segura de la Red de Área Local (LAN) sobre una red pública o no controlada, como Internet.

0 Prefacio

Control de versión y administración del documento:

Es responsabilidad del lector asegurarse de tener la última versión de este documento. Cualquier pregunta acerca del mismo deberá dirigirse con el propietario de este documento.

Autor de este documento:

El contacto principal para preguntas y observaciones acerca de este documento es:
Dirección General de Informática y Sistemas
informatica.sistemas@iepcgro.mx

Confidencialidad:

La información contenida en este documento deberá tratarse como información privada y confidencial. Esta información no deberá divulgarse a otras personas que no estén involucradas en el proyecto **"Programa de Resultados Electorales Preliminares"** para el Proceso Electoral Ordinario de Diputaciones Locales y Ayuntamientos 2023-2024 del estado de Guerrero**.**

1 Introducción

El presente documento fue elaborado con la finalidad de presentar la metodología y mecanismos de seguridad de la información a implementar en la solución PREP en el Proceso Electoral Local Ordinario 2023-2024 del estado de Guerrero. Estos mecanismos tienen como objetivo principal salvaguardar la integridad, disponibilidad y confidencialidad de la información e infraestructura tecnológica, fundamentándose en las mejores prácticas.

2 Plan de seguridad

La seguridad con la cual se maneja la información es uno de los puntos más importantes de esta solución, se propone el siguiente plan de fortalecimiento de seguridad para garantizar el flujo e integridad de la información, se compone de dos esquemas diferentes, el primero soportará el proceso de preparación a la elección y el segundo con mayor robustez para soportar el día de la jornada electoral (PREP).

2.1 Arquitectura de seguridad

Los sistemas informáticos por utilizar en el proceso PREP se habilitarán en un sistema de nube híbrida, combinando una nube privada, infraestructura en SITIO dentro del **IEPC Guerrero,** con seguridad perimetral definida por firewalls, y un servicio de nube pública con seguridad perimetral en nube.

Para la comunicación interna se usarán VPN con encriptación de datos de 256 bits. Además, para evitar la saturación de servidores, se utilizarán balanceadores de carga para que distribuyan las peticiones de los usuarios. En los centros de datos internamente se operará con VLAN privadas, y dentro de estas redes habrá firewalls que evitarán que usuarios entren en la red interna de los centros de datos utilizando Intrusion Prevention System (IPS) e Intrusion Detection System (IDS).

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 40 puntos de presencia a nivel mundial y capacidad de entregar 20 Gbps de sitio web “limpio”. 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.

2.2 Estructura del modelo de seguridad

Se propone la utilización de dos centros de datos distintos para garantizar la operación de los sistemas en su totalidad, debido a que los datos se guardan inicialmente en el Centro de Datos 1 (CD1) y este, a la vez, replica de manera inmediata los datos capturados a un centro de datos remoto de contingencia (CD2). Esta replicación es en tiempo real para los datos más críticos, tales como bases de datos, actas digitalizadas, sesiones, etcétera, y de 60 segundos en los datos de menor nivel, tales como contenidos estáticos de servidores de publicación, servicios secundarios, etcétera.

Con esta metodología se logrará tener un ambiente de alta disponibilidad con capacidad de continuidad en los procesos principales, tales como servidores de almacenamiento y captura de actas, servidores de bases de datos y servidores de difusión pública de resultados.

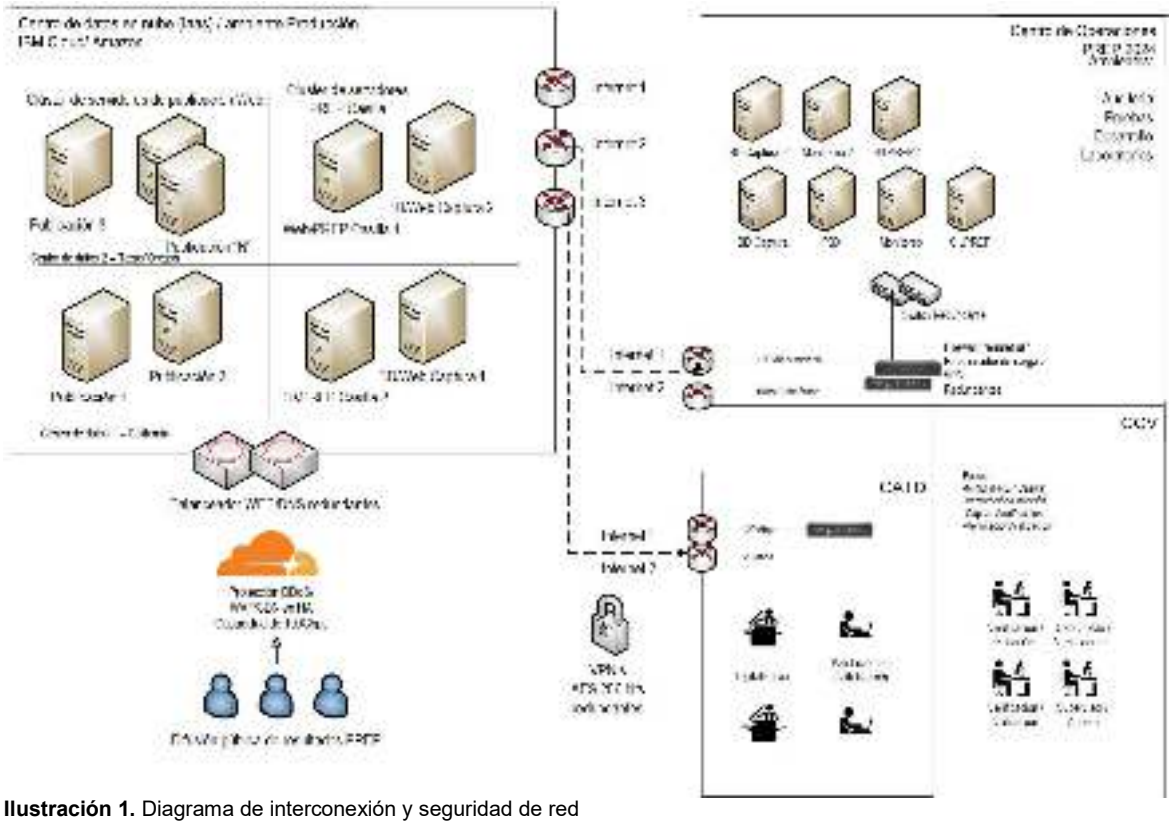

Ilustración 1. Diagrama de interconexión y seguridad de red

2.3 Estrategia de gestión de riesgo

Para asegurar que existan controles adecuados para reducir el riesgo por amenazas identificadas y ataques de seguridad, hacia el centro de datos y páginas web oficiales, se propone generar un análisis de nivel y probabilidad de impacto de cada contingencia clasificada por tipo y a su vez la realización de planes de respuesta con las medidas pertinentes a utilizar inmediatamente después de identificada una amenaza.

3 Análisis de Riesgos

Para la eficiente gestión de riesgos, se toman los siguientes criterios o acciones:

Evaluación de riesgos: Antes de siquiera empezar con la detección de riesgos, se debe tener en claro cuál es el nivel de riesgo que es posible aceptar, para lograr esto, se tiene una metodología que combina la criticidad de que se materialice un

riesgo, o bien, su nivel de contingencia, en conjunto con su probabilidad de ocurrencia, en el caso del proyecto PREP, no se aceptará ningún riesgo de nivel Alto y en conjunto con el OPL se definirá cuales riesgos de nivel Medio no son aceptables, por su parte, los riesgos de nivel bajo, pueden ser aceptados a menos que alguna parte interesada exija lo contrario.

Detección de riesgos: El IEPC Guerrero tiene una metodología de detección de riesgos en la que se dividen de la siguiente forma: por hardware o infraestructura, software o sistemas, recursos humanos, sitios o ubicaciones de trabajo, procesos y donde se plasma el área en el que podría materializarse el riesgo.

Solución y documentación: En caso de ser un riesgo que exija ser tratado de acuerdo con la evaluación de riesgos, se debe, verificar la documentación existente para encontrar medidas preventivas o correctivas, y adecuarlas a la situación específica, en el caso de que sea un riesgo que se materialice, el grupo coordinador movilizará al grupo de respuesta correspondiente, y una vez finalizada, documentará la solución para futuras referencias.

3.1 Niveles de contingencia

La clasificación de contingencia se realizó en base al impacto que podría ocurrir en el resultado del proyecto PREP Guerrero 2024:

NIVEL A (Contingencia Alta): En los posibles eventos a ocurrir de mayor desastre, los cuales afecten de manera muy significativa el cumplimiento del objetivo del PREP.

NIVEL M (Contingencia Media): En los posibles eventos a ocurrir de desastre, bloqueo o interrupción a escala que afecte a más de un equipo, usuario o grupo.

NIVEL B (Contingencia Baja): En los posibles eventos a ocurrir, en donde se presente que la contingencia solo afecta a un equipo, a un usuario, a un dispositivo, en donde su solución sea rápida y sencilla.

3.2 Probabilidad de ocurrencia

Además de clasificar el impacto de las contingencias en el proceso PREP Guerrero 2024, se clasificó por probabilidad de ocurrencia:

Probabilidad A (Alta): Las contingencias con mayor probabilidad de ocurrencia.

Probabilidad M (Media): Las contingencias con media probabilidad de ocurrencia.

Probabilidad B (Baja): Las contingencias con menor probabilidad de ocurrencias.

3.3 Evaluación de riesgo

Una vez obtenido el nivel de contingencia de cada riesgo y su nivel de ocurrencia, se evaluarán de la siguiente forma:

		Nivel de contingencia		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto

Tabla 1. Evaluación de riesgo

3.4 Hardware

CONTINGENCIA HARDWARE	NIVEL	PROBABILIDAD DE OCURRENCIA	CATD	IAAS	COPREP / CCV	IEPC
Fallo de laptop	B	M	X		X	X
Falla del modem	B	M	X	X	X	X
Falla del teclado, ratón o monitor	B	B	X		X	X
Falla VPN	B	M	X	X		
Falla conexión a internet	M	M	X	X	X	X
Falla de escáner	B	M	X			
Hackeo hosting	M	B		X	X	
Caída temporal del servidor por falla mecánica	M	M		X	X	
Pérdida total de un servidor	A	B		X	X	X
Falla total o parcial del cableado	M	B	X	X	X	
Pérdida total o parcial de las estaciones de trabajo	M	B	X	X	X	X
Falla en líneas telefónicas	B	M	X		X	X
Lentitud por causa de hardware (equipo muy lento)	B	M	X		X	X

CONTINGENCIA HARDWARE	NIVEL	PROBABILIDAD DE OCURRENCIA	CATD	IAAS	COPREP / CCV	IEPC
Falla en concentradores, switch o ruteador	B	M	X	X	X	X
Fallo en las pantallas para presentación de resultados	B	B			X	
Caída de firewall	M	B		X		X
Reconfiguración de equipo (escáner, PC)	M	B	X			

Tabla 2. Hardware

3.5 Software

CONTINGENCIA SOFTWARE	NIVEL	PROBABILIDAD DE OCURRENCIA	CATD	IAAS	COPREP / CCV
Error de conexión al ejecutar los sistemas PREP	A	B	X	X	
Error en los sistemas del PREP	A	B	X		X
Fallo del sistema operativo	B	B	X		X
Fallo en el sistema de verificación	A	B	X		
Virus en equipos de cómputo	B	B	X		X
Fallo del antivirus	M	B	X		
Lentitud en el sistema de captura PREP	M	M			X
Falla en el sistema de monitoreo	M	B			X
Información y resultados no concisos, ni lógicos	A	B			X
Error en nombre de usuario y contraseña	B	M	X		X
Perdida de nombre de usuario por parte de administradores, Help Desk y soporte técnico	B	M			X
No abre el navegador	M	M	X	X	X

Tabla 3. Software

3.6 Recursos humanos

CONTINGENCIA RECURSOS HUMANOS	NIVEL	PROBABILIDAD DE OCURRENCIA	CATD	IAAS	COPREP / CCV	IEPC
Capturista o digitalizador no conoce el sistema	B	M	X		X	
Falta uno de los capturistas o digitalizadores	B	M	X		X	
Indisposición del personal durante la jornada	B	M	X		X	X
Conflicto entre el personal	B	B	X		X	X
Cansancio excesivo por parte del personal que impidan o frenen el desarrollo normal de sus funciones	B	B	X		X	X
No se permite acceso a personal de captura	B	B			X	
Amenazas graves contra la seguridad del personal	M	B	X		X	X
Extensión del horario de trabajo en la madrugada.	B	M	X		X	X
Error en captura	B	A			X	
Captura errónea intencional	B	B			X	
Lentitud en captura de actas	B	A			X	
Borrado de archivos (intencional o no)	B	B			X	
Ausencia de Personal en General	M	M	X		X	

CONTINGENCIA RECURSOS HUMANOS	NIVEL	PROBABILIDAD DE OCURRENCIA	CATD	IAAS	COPREP / CCV	IEPC
No conocer el rol a desempeñar	A	M	X		X	X
Ausencia por Enfermedad o Accidente	A	A	X		X	X

Tabla 4. Recursos humanos

3.7 Sitios o ubicaciones de trabajo

CONTINGENCIAS SITIOS O UBICACIONES DE TRABAJO	NIVEL	PROBABILIDAD DE OCURRENCIA	CATD	IAAS	COPREP / CCV
Falla de energía eléctrica	M	M	X	X	X
Situación de alerta en oficinas por el clima	A	B	X	X	X
Situación de alerta en oficinas por incendio	A	B	X	X	X
Situación de alerta por asalto en oficinas	A	B	X		X
Toma de instalaciones en oficinas	A	B	X		X
Ubicación o lugar indisponible	A	B	X		X
Robo de equipo	M	B	X		X

Tabla 5. Sitios o ubicaciones de trabajo

3.8 Proceso

CONTINGENCIA PROCESO	NIVEL	PROBABILIDAD DE OCURRENCIA	CATD	IAAS	COPREP / CCV
Los paquetes electorales y sobres del PREP no llegan a las oficinas distritales	M	M	X		
Extravío de paquete electoral y sobres PREP	M	M	X		
Llenado de Bolsa PREP Incorrecto	M	M	X		
Acta escaneada y capturada con incidencias	A	B	X		
Desconocimiento de incidencias en las Actas	A	B			X
Desconocimiento de los roles	A	B	X		X

Tabla 6. Proceso

3.9 Mecanismo de seguridad

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

3.9.1 Control de usuarios y contraseñas con privilegios de operación

Al ser el PREP un sistema en línea, es necesario que cuente con un mecanismo de acceso, por lo cual 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 privilegios de operación en las cuentas de usuario que se generen, contemplando diversos aspectos, como, por ejemplo, un usuario de digitalización e identificación del CATD del Distrito V no podrá digitalizar e identificar actas e información del CATD del Distrito IV, los usuarios de tipo “consulta”, como su nombre lo indica, no podrán capturar información, entre otros.

Cabe destacar que los equipos de cómputo utilizados en PREP, en su totalidad cuentan con actualizaciones al día en sistema operativo, hardware y antivirus, asimismo se cuenta con documentos para la administración y configuración de los dispositivos de comunicaciones, servidores y base de datos para evitar vulnerabilidades en su operación, siendo señalados en el plan de habilitación y desinstalación y plan de capacitación y entrenamiento.

Para establecer las contraseñas a utilizar, se contará con una longitud y nivel de complejidad mínimo que deberá cumplir dicha contraseña, y se renovará previo al inicio de cada ejercicio, simulacro y jornada electoral.

Complementando la seguridad de los equipos de cómputo a utilizarse en el PREP, se inhabilitan los puertos USB de cada uno de los dispositivos, así como la inhabilitación y restricción de las tarjetas de red inalámbrica (Wi-Fi) y Bluetooth y bandejas lectoras de CD/DVD.

Este procedimiento evita filtración de información y protegen 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 de dichos usuarios se generarán desde un sistema central, el cual seguirá 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.

Además, para garantizar la seguridad y la estabilidad de los servicios principales en la zona privada, se utilizarán las últimas versiones estables que han pasado por la fase de pruebas del IEPC Guerrero, de los siguientes componentes:

Sistemas operativos:

- Ubuntu Linux 22.04 LTS (Soporte extendido).

- Equipos de cómputo: Windows 11 (Con las últimas actualizaciones de seguridad)
- Equipos celulares: Android 13

Motores de bases de datos
- MariaDB 10.4.28

Framework de desarrollo
- Laravel 10.10.0
- Angular 16.0.4
- Python 3.9.18

Lenguaje de programación
- PHP 8.2.15

Estas medidas contribuyen a la protección contra amenazas más avanzadas, la gestión proactiva de vulnerabilidades y la utilización de tecnologías actualizadas con soporte técnico activo.

3.9.2 Comunicación cifrada de información

Para fortalecer los mecanismos de envío de la información a través de Internet, se implementarán firewalls con capacidad de encriptación de 256 bits, con esto generando canales seguros entre los CATD's, CCV's y Centro de Operación, 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 sistemas de comercio electrónico y servicios bancarios en línea.

3.9.3 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 OPL 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 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.

El almacenamiento de la información proveniente de los CATD’s, se realizará en al menos dos servidores locales que trabajan en 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.

3.9.4 Mecanismos de redundancia de información y comunicación

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.

3.9.5 Bitácora de operaciones

Todo sistema de captura con múltiples usuarios debe contar con un control o bitácora de operaciones realizadas en el sistema, que incluya 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.

3.9.6 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 100Gbps, 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 40 puntos de presencia a nivel mundial y capacidad de entregar al menos 20Gbps de sitio web “limpio”.

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.

3.9.7 Listado de verificación de seguridad

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

3.9.8 Seguridad de los datos

Para realizar el proceso PREP la Dirección General de Informática y Sistemas hará la configuración y pruebas necesarias de los siguientes equipos informáticos en cada CATD:

- 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 concentrador de red: Se interconectarán los equipos de cómputo y tecnológicos para crear una red LAN.
- Cableado de red: Todos los equipos de cómputo se comunicarán mediante cableado Ethernet categoría 6 en los CATD y CCV.

3.10 Seguridad física en CATD y CCV

- El inmueble debe de 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 dañe 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.

- Conexiones eléctricas suficientes para la conexión de los equipos informáticos: Se debe de entregar una conexión de corriente eléctrica regulada y aterrizada a tierra, la cual se conectará al UPS.

3.11 Seguridad de personal

3.11.1 Identificaciones y detección de intrusos

Se implementará una estrategia para asegurar que el acceso a los CATD sea restringido a solo el personal autorizado por **IEPC Guerrero.** Se mantendrá el registro de los accesos, desde el registro por parte del personal de seguridad al acceso a las instalaciones de los Consejos Distritales Electorales donde se ubican los CATD, llevando una bitácora de acceso, además de la revisión de los registros para identificar anomalías.

Para tener una mayor seguridad en los centros, el personal que se encuentre dentro de cada centro deberá portar su identificación oficial, la cual tiene en su diseño: en la parte frontal, el logo del **IEPC Guerrero**, fotografía del portador, nombre y puesto; y en la parte trasera de la identificación, el código QR, firma de autorización y logo del **IEPC Guerrero.**

Tabla 1. Diseño de gafetes

No se permitirá el uso de dispositivos móviles de comunicación o fotográficos al interior de las instalaciones, salvo el autorizado por el **IEPC Guerrero.**

3.11.2 Seguridad en el acceso a la aplicación móvil

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

- Uso de token (el token tiene 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 son root (para PREP Casilla).
- 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.

- Las digitalizaciones se encriptarán en SHA: 256 (HASH) el cual se genera al digitalizar el acta 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 estos 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.
- Los celulares estarán restringidos 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.
- El personal operativo tendrá el siguiente proceso para:
- 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 el cual 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 para terminar el envío de imágenes.

4 Plan de concientización

4.1 Introducción

El plan de concientización es un programa formal que tiene como propósito capacitar y sensibilizar a los colaboradores del IEPC Guerrero en materia de las posibles amenazas (principalmente las de amenazas de seguridad de la información) y como gestionarlas, para ello este plan se estructura de la siguiente manera: Objetivo, alcance, situación actual, materiales de capacitación, plan de trabajo, reporte de situación final.

4.2 Objetivo

El objetivo del presente plan de concientización es que las y los usuarios que intervienen en el PREP, de acuerdo con sus atribuciones, puedan conocer los riesgos y las amenazas que enfrenta el Programa, así como saber la forma en que

pueden apoyar para minimizar dichos riesgos o prevenir algún incidente de seguridad.

4.3 Alcance

El presente plan de concientización abarca desde la definición de la situación actual a través de encuestas y/o pruebas de conocimiento en materia de seguridad de la información, pasando posteriormente por capacitación y concientización hasta la evaluación del personal capacitado con el objetivo de medir la efectividad de la capacitación.

Así mismo, el alcance especifico en la capacitación es el siguiente:

- Sensibilización sobre riesgos de seguridad de la información.
- Promoción de buenas prácticas.
    - Desarrollo seguro.
    - Herramientas y técnicas de configuración segura de servicios digitales.
    - Gestión de incidentes.
    - Planes de seguridad y continuidad.
- Divulgación de políticas.
- Cumplimiento normativo.

Es importante señalar que no todos los colaboradores llevarán la misma, capacitación, ya que, los contenidos por impartir dependerán del rol de cada colaborador en el proyecto.

4.4 Situación actual

Para que el plan de concientización tenga la efectividad deseada, es crucial entender las necesidades de capacitación que tienen los colaboradores, mismas que se buscarán comprender a través de la realización de una encuesta de conocimientos en materia del PREP, modelo de servicio y seguridad de la información, a continuación, se puede observar el cuestionario planteado:

1. ¿Qué es el PREP?
    a. Programa de Recuento Electoral Paralelo.
    b. Programa de Resultados Electorales Preliminares.
    c. Proceso de Registro de Electores y Participación.
    d. Ninguna de las anteriores.

2. ¿Alguna vez has sido víctima de algún hackeo en tus dispositivos laborales o personales? De haberlo sido y si está en tus posibilidades, detalla el acontecimiento y si tuvo o no solución y su causa más probable.
    a. Si.
    b. No.
    c. No, pero conozco alguien que sí.

    Explicación de la situación:
3. ¿En tus palabras, como definirías la seguridad de la información?
4. ¿Cuáles son los 3 pilares de seguridad de la información?
    a. Confidencialidad, Disponibilidad e Integridad.
    b. Confidencialidad, Privacidad y Veracidad.
    c. Información, Confidencialidad, Datos.
5. ¿Qué conoces como phishing?
6. ¿Has vivido situaciones en las que hayas tenido que aplicar algún plan de seguridad y continuidad? Si es así y está dentro de tus posibilidades, detalla la situación.
    a. Si.
    b. No.
    c. Detalla la situación:
7. Subraya los equipos que sabes utilizar:
    a. Extintor de incendios.
    b. Cámaras de vigilancia.
    c. Planta generadora de energía eléctrica.
    d. IDS e IPS.
    e. Controles de acceso físico.
    f. Software de antivirus.
    g. Firewall.
    h. Herramientas de criptografía.
    i. Herramientas de gestión de contraseñas.
8. ¿Qué medidas de seguridad de la información has tomado?
9. ¿Qué métodos para la evaluación de riesgos conoces?
10. ¿Estas familiarizado con alguna metodología de gestión de riesgos?

4.5 Materiales de capacitación

El IEPC Guerrero dependiendo del tipo de capacitación, brindará los siguientes materiales de capacitación:

- Presentaciones en PowerPoint.
- Equipo de cómputo.
- Acceso a internet y servicios de correo y mensajería.

4.6 Plan de trabajo

Personal por capacitar	Contenido	Actividades por desarrollar	Recursos y materiales didácticos	Tiempo	Responsable
COPREP, Agentes de Soporte Técnico, Agentes de Personal y Supervisor Logístico	-Sensibilización sobre riesgos de seguridad de la información. -Promoción de buenas prácticas. -Gestión de incidentes. -Planes de seguridad y continuidad.	-Presentación mediante técnica grupal, a elección del facilitador. -Sesión de preguntas y respuestas. -Aplicación de cuestionario de opción múltiple. -Recapitulación del tema completo.	-PowerPoint con el tema completo. -Prueba objetiva. (cuestionario con 10 ítems, de opción múltiple) -Pantalla para proyección. -Un proyector. -Equipo de cómputo.	3 horas	Coordinador de Software e Implementación.
Personal Operativo (Coordinadores y Supervisores de CATD y en su caso CCV,	-Sensibilización sobre riesgos de seguridad de la información. -Promoción de buenas prácticas. -Gestión de incidentes. -Planes de seguridad y continuidad.	-Presentación mediante técnica grupal, a elección del facilitador. -Sesión de preguntas y respuestas. -Aplicación de cuestionario de opción múltiple. -Recapitulación del tema completo.	-PowerPoint con el tema completo. -Prueba objetiva. (cuestionario con 10 ítems, de opción múltiple) -Pantalla para proyección. -Un proyector. -Equipo de cómputo.	3 horas	Coordinador de Software e Implementación.
capturistas / verificadores, y digitalizadores	-Sensibilización sobre riesgos de seguridad de la información. -Promoción de buenas prácticas. -Gestión de incidentes. -Planes de seguridad y continuidad.	-Presentación mediante técnica grupal, a elección del facilitador. -Sesión de preguntas y respuestas. -Aplicación de cuestionario de opción múltiple. -Recapitulación del tema completo.	-PowerPoint con el tema completo. -Prueba objetiva. (cuestionario con 10 ítems, de opción múltiple) -Pantalla para proyección. -Un proyector. -Equipo de cómputo.	3 horas	Coordinador de Software e Implementación.
Acopiadores	-Sensibilización sobre riesgos de seguridad de la información. -Promoción de buenas prácticas. -Gestión de incidentes. -Planes de seguridad y continuidad.	-Presentación mediante técnica grupal, a elección del facilitador. -Sesión de preguntas y respuestas. -Aplicación de cuestionario de opción múltiple. -Recapitulación del tema completo.	-PowerPoint con el tema completo. -Prueba objetiva. (cuestionario con 10 ítems, de opción múltiple) -Pantalla para proyección. -Un proyector. -Equipo de cómputo.	2 horas	Coordinador de Software e Implementación.

Tabla 2. Plan de trabajo

4.7 Modelo de capacitación

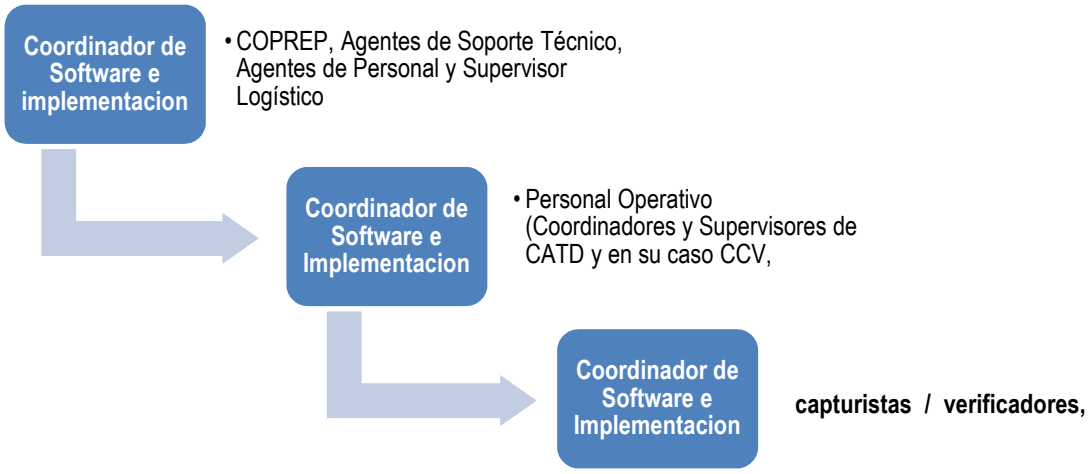

Ilustración 2. Modelo de capacitación

4.8 Cronograma de actividades

Puestos	Fechas
PUESTOS POR CAPACITAR	**FECHA EN QUE SE TIENE PLANEADO CONTRATAR Y CAPACITAR**
COPREP, Agentes de Soporte Técnico, Agentes de Personal y Supervisor Logístico	5 de abril de 2024
Personal Operativo (Coordinadores y Supervisores de CATD y en su caso CCV,	5 de abril de 2024
capturistas / verificadores, y digitalizadores	18 de abril de 2024
Acopiadores	6 de mayo de 2024

Tabla 3. Cronograma de actividades

4.9 Reporte de situación final

Para evaluar la efectividad del plan de concientización se realizará nuevamente una encuesta a los colaboradores que ya fueron capacitados, donde se incluirán los mismos reactivos de la encuesta inicial, más algunos reactivos extra, observándose de la siguiente manera:

1. ¿Qué es el PREP?
    a. Programa de Recuento Electoral Paralelo.
    b. Programa de Resultados Electorales Preliminares.
    c. Proceso de Registro de Electores y Participación.
    d. Ninguna de las anteriores.

2. ¿Alguna vez has sido víctima de algún hackeo en tus dispositivos laborales o personales? De haberlo sido y si está en tus posibilidades, detalla el acontecimiento y si tuvo o no solución y su causa más probable.
    a. Si.
    b. No.
    c. No, pero conozco alguien que sí.

    Explicación de la situación:
3. ¿En tus palabras, como definirías la seguridad de la información?
4. ¿Cuáles son los 3 pilares de seguridad de la información?
    a. Confidencialidad, Disponibilidad e Integridad.
    b. Confidencialidad, Privacidad y Veracidad.
    c. Información, Confidencialidad, Datos.
5. ¿Qué conoces como phishing?
6. ¿Has vivido situaciones en las que hayas tenido que aplicar algún plan de seguridad y continuidad? Si es así y está dentro de tus posibilidades, detalla la situación.
    a. Si.
    b. No.
    c. Detalla la situación:
7. Subraya los equipos que sabes utilizar:
    a. Extintor de incendios.
    b. Cámaras de vigilancia.
    c. Planta generadora de energía eléctrica.
    d. IDS e IPS.
    e. Controles de acceso físico.
    f. Software de antivirus.
    g. Firewall.
    h. Herramientas de criptografía.
    i. Herramientas de gestión de contraseñas.
8. ¿Qué medidas de seguridad de la información has tomado?
9. ¿Qué métodos para la evaluación de riesgos conoces?
10. ¿Estas familiarizado con alguna metodología de gestión de riesgos?
11. ¿Cómo se evalúan los riesgos En IEPC Guerrero de acuerdo con su nivel de contingencia y su probabilidad de ocurrencia?
12. ¿Cuál es la forma correcta de actuar desde tu rol ante una incidencia de nivel bajo?
13. ¿Cuál es la forma correcta de actuar desde tu rol ante una emergencia?