Esquema de arquitectura y seguridad.


Esquema de operación
Medidas de Seguridad en los CATD
Medidas de Seguridad en los CRID
Medidas de Seguridad en RedINE
Plan de Continuidad de la Operación
Auditoría de Seguridad UNAM
Colaboración con organizaciones externas

Esquema de Operación

1 Acopio

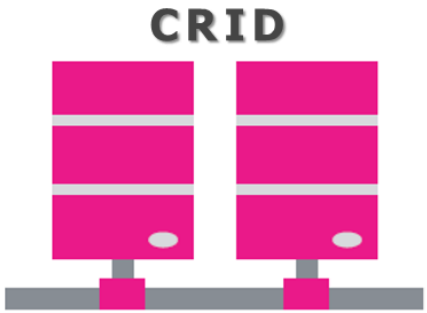
Impresión de fecha y hora de acopio con reloj checador

2 Digitalización

Etiquetado QR en el acta y digitalización (MCAD)

3 Registro

Registro de la imagen del acta y preparación de envío para su captura de datos



4 Captura

Captura y recaptura de datos, envío al CRID

5 Verificación

Revisión de datos y de imagen.

6 Almacenaje

Una vez terminadas las actividades en el CATD se procedera al resguardo de las actas

Publicación

Informar oportunamente al Consejo General, Partidos Políticos, Medios de comunicación y a la ciudadania


Esquema de operación
Medidas de Seguridad en los CATD
Medidas de Seguridad en los CRID
Medidas de Seguridad en RedINE
Plan de Continuidad de la Operación
Auditoría de Seguridad UNAM
Colaboración con organizaciones externas

Centros de Acopio y Transmisión de Datos

Dispositivos de comunicaciones

- Esquema de conexión de alta disponibilidad.
- Segmentación lógica del tráfico del CATD.
- Administración remota sólo sobre canales cifrados.
- Controles contra ataques de negación de servicio (seguridad a nivel de puertos, configuración contra ataques de suplantación, monitoreo de tablas ARP).
- Configuración de Dispositivos basada en mejores prácticas en materia de seguridad (recomendaciones NIST, CERT, SANS, CIS).

Centros de Acopio y Transmisión de Datos

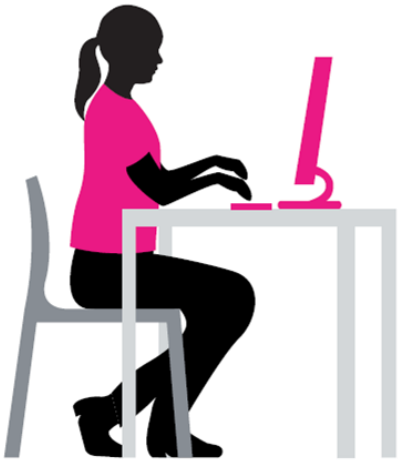
Monitor de Captura de Actas Digitalizadas (MCAD)

- Sistema operativo Microsoft Windows el cuál cuenta con la configuración de seguridad:
  a. Medidas y controles contra software malicioso y código móvil.
  b. Uso de contraseña.
  c. Políticas de puesto de trabajo despejado y bloqueo de pantalla.
  d. Aislamiento del sistema de digitalización mediante un perfil.
- Mecanismo de autenticación de 2 factores para utilizar el software de digitalización de actas.

Centros de Acopio y Transmisión de Datos

Terminales de Captura de Acta (TCA)

- Sistema operativo Linux Fedora 20 con configuración de seguridad de acuerdo a buenas prácticas internacionales.
- Mecanismos de autenticación de 2 factores para utilizar el software de Captura de acta.



Centros de Acopio y Transmisión de Datos

Dispositivos criptográficos.

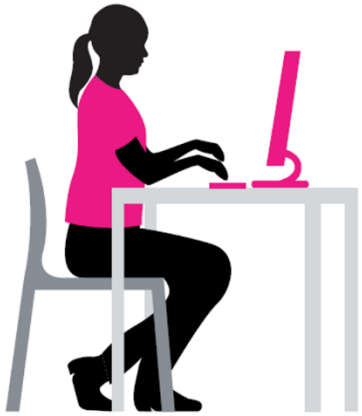
- Cumple con estándares de seguridad FIPS 140-2 Nivel 3 para proteger las claves que contiene.
- La interfaz USB lo hace compatible con cualquier PC.
- Se puede aprovechar la optimización de los algoritmos criptográficos en hardware.

Centros de Acopio y Transmisión de Datos

Proceso de Digitalización.

- Autenticación de coordinador mediante el dispositivo criptográfico.
- Automatización de la captura de las datos de las actas mediante el uso de Códigos QR (id estado, id distrito, tipo de casilla, id casilla, número de acta).
- Generación de un identificador único asociado a cada archivo del Acta digitalizada (SHA1).
- Uso del algoritmo RSA para realizar el firmado electrónico de todas las transacciones. RSA es el estándar criptográfico aceptado a nivel mundial para firmas electrónicas.

Centros de Acopio y Transmisión de Datos



Proceso de Captura.

- Autenticación de coordinador, supervisor y capturista mediante el dispositivo criptográfico.
- Proceso de doble captura.
- Todas las transacciones se almacenan en la TCA para retransmisión o auditorías posteriores.
- Uso del algoritmo RSA para realizar el firmado electrónico de todas las transacciones. RSA es el estándar criptográfico aceptado a nivel mundial para firmas electrónicas.


Esquema de operación
Medidas de Seguridad en los CATD
Medidas de Seguridad en los CRID
Medidas de Seguridad en RedINE
Plan de Continuidad de la Operación
Auditoría de Seguridad UNAM
Colaboración con organizaciones externas

Centro de Recepción de Imágenes y Datos

Estrategia de Protección

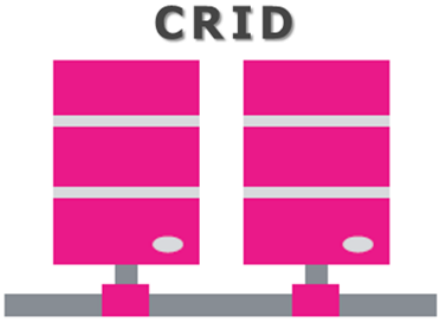
Dispositivos de Comunicaciones (dedicados a Seguridad)

- Uso de dispositivos de detección de intrusos a nivel de red (Network IDS) y de servidores (host IDS).
- Redundancia de dispositivos de detección de intrusos.
- Configuración de los IDS de acuerdo al tipo de tráfico esperado en el CRID.
- Uso de dispositivos de filtrado de paquetes de red (firewalls) en el perímetro del CRID.
- Redundancia de los dispositivos de filtrado de paquetes de red.
- Configuración de política restrictiva.

Centro de Recepción de Imágenes y Datos

Estrategia de Protección

Dispositivos de Comunicaciones (conectividad)



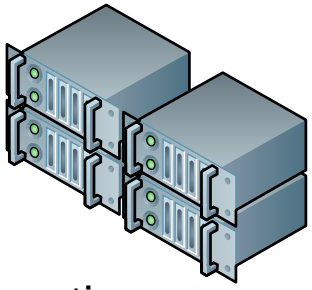
- Esquema de redundancia de enlaces para garantizar alta disponibilidad.
- Segmentación del tráfico utilizando redes virtuales.

- Monitoreo proactivo del comportamiento del tráfico de red.
- Configuración de los dispositivos de red basada en las mejores prácticas en materia de seguridad (recomendaciones NIST, CERT, SANS, CIS).

Centro de Recepción de Imágenes y Datos

Estrategia de Protección

Servidores de Aplicaciones y Publicación



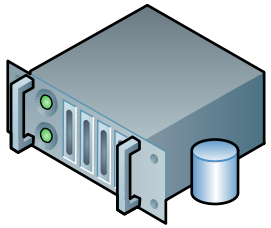
- Esquema de cluster para garantizar alta disponibilidad.
- Personalización del núcleo del sistema operativo.
- Filtrado de tráfico de red a nivel del núcleo del sistema operativo.
- Uso de contraseñas de una sola vez (one time password) para administradores.
- Configuración de los servidores basada en las mejores prácticas en materia de seguridad (recomendaciones NIST, CERT, SANS, CIS).

Centro de Recepción de Imágenes y Datos

Estrategia de Protección

Servidores de bases de datos

- Uso de tecnología de Oracle para garantizar la alta disponibilidad del servicio y la réplica de datos entre el CRID primario y el CRID secundario.
- Control de acceso a nivel del manejador de la base de datos.



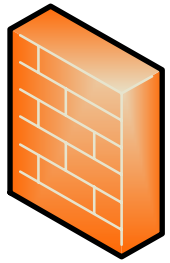
- Monitoreo proactivo del estado de la base de datos.
- Configuración de la base de datos basada en las mejores prácticas en materia de seguridad (recomendaciones NIST, CERT, SANS, CIS).


Análisis de riesgos
Medidas de Seguridad en los CATD
Medidas de Seguridad en los CRID
Medidas de Seguridad en RedINE
Plan de Continuidad de la Operación
Auditoría de Seguridad UNAM
Colaboración con organizaciones externas

Red Nacional de Informática (RedINE)
Estrategia de Protección

Control de Acceso a nivel de red

- Redes internas segmentadas lógicamente.
- Zonas delimitadas por firewalls (DMZ, Intranet, Internet).
- Validación de direcciones MAC a nivel de switch.



Control de Acceso a nivel de servidor

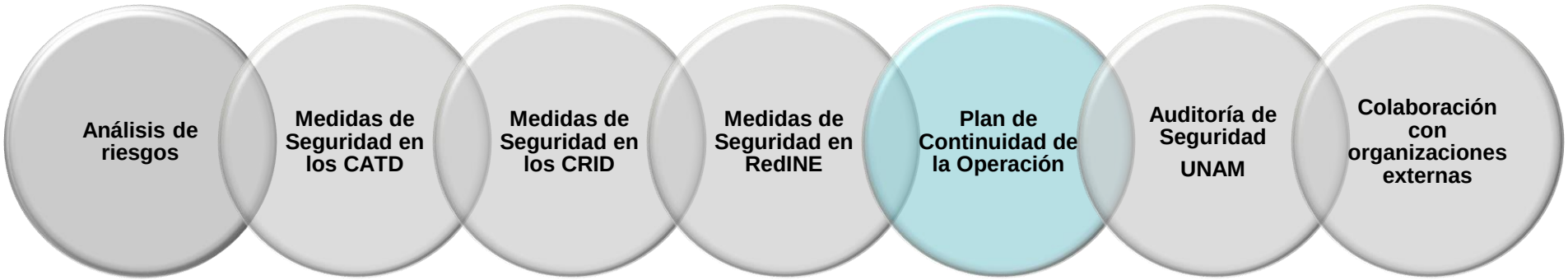
- Delimitación de privilegios y ejecución de tareas.
- Detectores de intrusos a nivel de servidor.
- Monitoreo de integridad de los componentes del sistema.

Red Nacional de Informática (RedINE)

Estrategia de Protección

Protección contra Código Malicioso

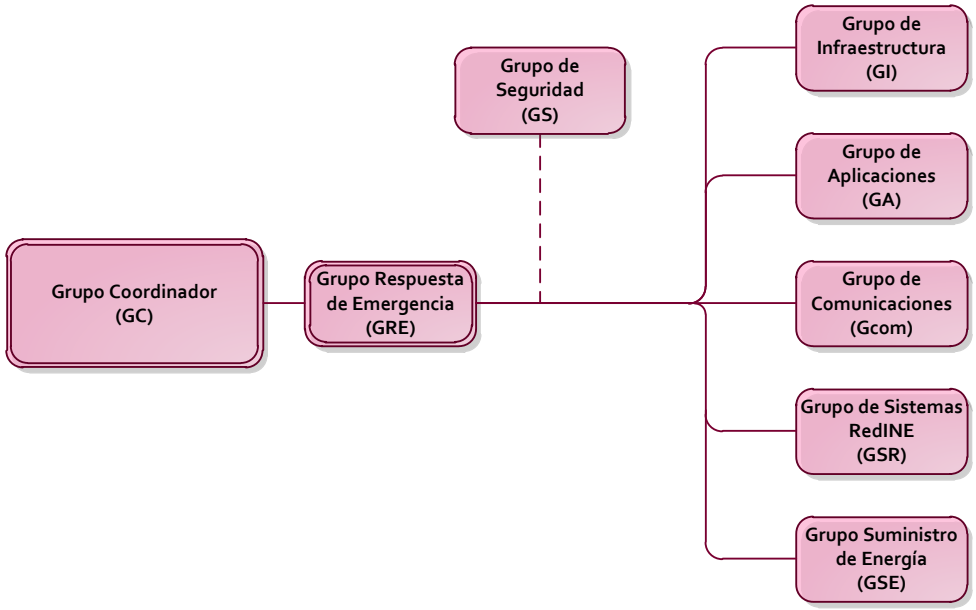
- Actualización continua del antivirus Institucional.
- Monitoreo y desarrollo de acciones ante noticias relacionadas con la explotación de vulnerabilidades en los sistemas.
- Mecanismos de bloqueo de correos portadores de código malicioso.
- Mecanismos de protección contra ataques de negación de servicio.
- Elaboración de material didáctico para actualización del sistema operativo y uso del antivirus Institucional.
- Revisión de tendencias en redes sociales.


Análisis de riesgos
Medidas de Seguridad en los CATD
Medidas de Seguridad en los CRID
Medidas de Seguridad en RedINE
Plan de Continuidad de la Operación
Auditoría de Seguridad UNAM
Colaboración con organizaciones externas

Plan de Continuidad de la Operación

Grupos de recuperación

- Los Grupos de Recuperación de Incidentes están conformados por personal directivo y operativo de las áreas de la Unidad Técnica de Servicios de Informática (UNICOM).



Plan de Continuidad de la Operación

Estrategias de Continuidad:

- Sitios espejo: CRID Primario y CRID Secundario
- Esquema de redundancia en los siguientes niveles:
  - ➢ Redundancia en infraestructura eléctrica.
  - ➢ Dispositivos internos.
    - ▪ Doble fuente de poder.
    - ▪ Arreglos de discos (RAID).
  - Equipos de Comunicaciones y Servidores.
    - ➢ Enlaces redundantes de comunicación.
    - ➢ Centralmente, grupos de clusters de servidores que permiten alta disponibilidad.

❑ A nivel CATD, existe equipo de comunicaciones de remplazo.

Plan de Continuidad de la Operación

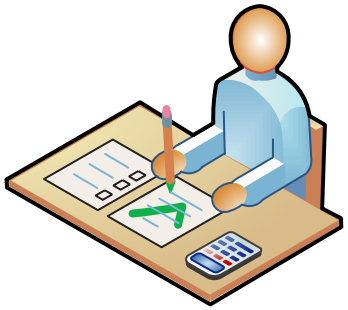
Estrategias de Continuidad:

- Apoyo por parte de Telmex
  - Asignación de trayectorias distintas en la infraestructura de comunicaciones
  - Asignación de cuadrillas para atender fallos de los enlaces de comunicaciones durante pruebas nacionales y el día de la jornada
- Apoyo por parte de la Comisión Federal de Electricidad
  - Revisión y mantenimiento a las acometidas eléctricas que corresponden a cada una de las Juntas Ejecutivas Distritales
  - Cuadrillas para atender fallos de energía durante pruebas nacionales y el día de la jornada electoral


Análisis de riesgos
Medidas de Seguridad en los CATD
Medidas de Seguridad en los CRID
Medidas de Seguridad en RedINE
Plan de Continuidad de la Operación
Auditoría de Seguridad UNAM
Colaboración con organizaciones externas

Auditoría de seguridad UNAM

- Auditoría de seguridad a la infraestructura de RedINE y del PREP
  - Pruebas de penetración a la Infraestructura tecnológica de RedINE
  - Pruebas de penetración a la Infraestructura tecnológica de. PREP
- Monitoreo y respuesta a incidentes PREP durante el día de la Jornada Electoral




Análisis de riesgos
Medidas de Seguridad en los CATD
Medidas de Seguridad en los CRID
Medidas de Seguridad en RedINE
Plan de Continuidad de la Operación
Auditoría de Seguridad UNAM
Colaboración con organizaciones externas

Colaboración Externa

Estrategia de protección

- Colaboración con el CERT de la UNAM a través del convenio de colaboración
- Participación de TELMEX
- Participación de CFE

Fortalecimiento de la difusión de los resultados del PREP

- Servicios terciados de publicación contratados por el INE

INE
Instituto Nacional Electoral