Programa de Resultados Electorales Preliminares (PREP)
Proceso Local Electoral 2020-2021

ANEXO TÉCNICO - Requisitos para la Auditoría Informática

ÍNDICE

INTRODUCCIÓN

En el marco de las actividades para la implementación y operación del Programa de Resultados Electorales Preliminares (PREP) para el Proceso Local Electoral 2020-2021 en el Estado de Baja California Sur, se requiere que se lleve a cabo una auditoría al sistema informático y a la infraestructura tecnológica del PREP, de conformidad con lo dispuesto en la sección cuarta, del capítulo II del Reglamento de Elecciones del INE, así como del título II, capítulo III, de su Anexo 13 relativo a los Lineamientos del PREP. Se deberá considerar en la auditoría los módulos operativos del sistema, incluyendo el aplicativo móvil “PREP Casilla”.

Para tal efecto, en el presente documento se describe el alcance que debe cumplir el proveedor de servicios seleccionado como ente auditor. Asimismo, se detallan los requerimientos de cada línea de trabajo que deberán considerarse durante el transcurso de la auditoría.

Las líneas de trabajo a considerar son:

1.1 Pruebas funcionales de caja negra al sistema informático del PREP Local 2021 y a la aplicación móvil que se utilizará para operar el mecanismo de digitalización de las Actas desde las casillas.”.
1.2 Validación del sistema informático del PREP y de sus bases de datos.
1.3 Análisis de vulnerabilidades a la infraestructura tecnológica.
1.4 Pruebas de negación de servicio al sitio web del PREP y al sitio oficial del Instituto.

ASPECTOS GENERALES DE LA AUDITORÍA

- El ente auditor deberá nombrar a un Auditor o Auditora Líder dentro de su equipo de trabajo, quien tendrá la responsabilidad de turnar los planes e informes señalados en el presente documento. De igual forma, dicha figura fungirá como el canal de comunicación del ente auditor con la Instancia interna para la coordinación del PREP del Instituto.
- A todo entregable señalado en las líneas de trabajo del presente documento, se deberá especificar la **Fecha de entrega** en el Plan de Trabajo que el ente auditor deberá entregar al inicio de sus trabajos.
- En lo que respecta a la **Forma de entrega** de los planes e informes, se deberán remitir de manera electrónica al correo ucsi@ieebcs.org.mx. A la par de lo anterior, los informes finales deberán ser entregados de manera impresa al Titular de la Instancia Interna de coordinación del PREP del Instituto.

1.1 PRUEBAS FUNCIONALES DE CAJA NEGRA AL SISTEMA INFORMÁTICO DEL PREP LOCAL 2021

Objetivo

El ente auditor deberá analizar el sistema informático del PREP mediante la realización de pruebas funcionales de caja negra, para evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares, conforme a lo establecido en el artículo 347, numeral 1, inciso a) del Reglamento de Elecciones.

Alcance

Como parte del alcance de las pruebas funcionales de caja negra el Instituto debe considerar aquellas etapas de su Proceso Técnico Operativo que estén instrumentadas a través del sistema informático, realizando los ajustes necesarios en relación con las actividades que se lleven a cabo a través de procesos o procedimientos cuya ejecución sea manual o que no considere el uso del sistema informático del PREP. En este sentido, se señalan a continuación los escenarios principales que deben incluirse como parte del alcance.

Las pruebas de caja negra deberán realizarse en términos de funcionalidad del sistema informático del PREP, y deberá considerar, al menos, los siguientes aspectos:

- Se debe analizar el funcionamiento de la aplicación en relación con las fases del proceso técnico operativo, considerando al menos, la digitalización, foliación, captura, verificación y publicación de resultados, mediante flujos completos e interacción entre los diversos módulos (escenarios principales). Se deberá incluir el análisis del funcionamiento del aplicativo PREP Casilla, mediante flujos completos e interacción entre los diversos módulos y fases mencionadas.
- Se debe verificar el cumplimiento de las especificaciones funcionales y requerimientos contenidos en la documentación técnica y normatividad aplicable que será proporcionada por el Instituto.

- Se debe verificar la correspondencia de la captura de los datos plasmados en las Actas PREP con los presentados en la publicación, mediante los distintos tipos de reportes desplegados por el PREP, considerando datos, imágenes y bases de datos.

  En dichos trabajos de validación de los reportes desplegados por el PREP, el ente auditor deberá revisar las pantallas de publicación del PREP, verificando el apego a las plantillas base de la interfaz del sitio de publicación de dicho sistema.

  Para realizar lo anterior, el ente auditor deberá aplicar las fases de digitalización (tanto por PREP Casilla como el módulo de Digitalización), foliación, captura y verificación a la totalidad de las Actas de Escrutinio y Cómputo de un distrito electoral en particular (elección de Diputaciones). Dicho distrito electoral se definirá previo al inicio de las pruebas de caja negra.

El alcance de las pruebas funcionales de caja negra deberá incluir los siguientes módulos del sistema informático del PREP:

I. Módulo de Digitalización, Foliación y Captura y Verificación

   a) Obtención de la imagen digital del acta (tanto PREP Casilla como digitalización desde los CATD).
   b) Captura de la información contenida en las Actas PREP
   c) Validación de la información capturada

II. Módulo de Publicación

   a) Revisión de la obtención de los resultados, así como de la emisión de reportes y su despliegue, de acuerdo con la documentación técnica y la normatividad aplicable.

Para realizar las pruebas, el Instituto deberá proporcionar los insumos de información necesarios, entre los que se encuentran, de manera enunciativa más no limitativa, los señalados en la sección “Condiciones Generales” del presente documento.

Entregables

El ente auditor deberá entregar los siguientes documentos derivados de los trabajos realizados:

Entregable	Descripción y Contenido	Criterios de Aceptación
Plan de pruebas funcionales de caja negra del sistema informático	Describe los elementos generales que deben considerarse para la realización de las pruebas funcionales de caja negra: • Introducción	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección

Entregable	Descripción y Contenido	Criterios de Aceptación
	• Objetivo • Alcance • Pruebas a aplicar • Planeación de las pruebas • Necesidades de ambiente • Casos de prueba • Datos de prueba • Criterios de pruebas • Administración de riesgos • Entregables	de descripción y contenido.
Informe preliminar de las pruebas funcionales de caja negra del sistema informático	Documento que contiene el detalle de cada una de las observaciones identificadas en la revisión y pruebas del sistema y que incluya, al menos: • Introducción • Metodología • Criterios utilizados para la auditoría • Metodología para clasificar los hallazgos • Observaciones detectadas, su nivel de impacto y recomendaciones que emite el Ente Auditor • Conclusiones Para tener un mejor seguimiento de las incidencias que reporte el ente auditor, se deberá considera una herramienta automatizada que permita realizar la gestión de dichas incidencias, tal como MantisBT. El ente auditor podrá proponer otro software que cumpla con las funcionalidades de seguimiento a bugs e incidentes de software. Cabe señalar que dicha herramienta será auxiliar solamente, siendo el Informe preliminar el medio oficial del ente auditor para la remisión de los resultados de las pruebas realizadas.	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.

Entregable	Descripción y Contenido	Criterios de Aceptación
	De igual forma el Instituto deberá informarle al ente auditor respecto de la versión del sistema de la cual se está realizando la auditoría, para efectos de tener un mejor control sobre qué versión se está realizando la auditoría.	
Informe final de las pruebas funcionales de caja negra del sistema informático	Documento que contiene el resultado final de las pruebas del sistema: • Introducción • Metodología • Criterios utilizados para la auditoría • Resumen ejecutivo • Resultados	Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.

Calendario de trabajo.

El calendario de actividades para esta línea de trabajo deberá establecer, de forma clara, los periodos para la ejecución de cada actividad y los avances esperados en cada periodo de trabajo.

1.2 VALIDACIÓN DEL SISTEMA INFORMÁTICO DEL PREP Y DE SUS BASES DE DATOS

Objetivo

Validar que el sistema informático del PREP que operará el día de la Jornada Electoral, corresponda al software auditado, así como que la base de datos se encuentre sin registros adicionales a los necesarios para que el sistema opere. La validación respecto a la correspondencia del software auditado y el utilizado en la operación del PREP, se tendrá que realizar al inicio, durante y al final de la operación del sistema informático del PREP.

Alcance

Especialistas del ente auditor deberán llevar a cabo un procedimiento técnico para verificar que los programas auditados se encuentren operando desde el inicio y hasta el cierre de operación del sistema informático del PREP, así como que la base de datos se encuentre debidamente inicializada. Dicho procedimiento deberá ser validado por el personal que el Instituto designe para tal efecto, contemplando los siguientes aspectos como mínimo:

- El procedimiento deberá contar con un diagrama de flujo.
- El procedimiento deberá incluir los roles y responsabilidades de los involucrados.
- El procedimiento deberá documentar como mínimo, las siguientes etapas:
    - Generación, obtención y validación de huellas criptográficas en SHA-256 del software PREP auditado.
    - Generación, obtención y validación de huellas criptográficas en SHA-256 del software PREP instalado en el ambiente productivo que operará el día de la Jornada Electoral.
    - Validación de la información inicial y final de la base de datos del PREP.
    - Constancia de hechos.

El procedimiento deberá realizarse el domingo 6 de junio de 2021 en las instalaciones del Instituto (o en su caso, del Centro de Captura y Verificación 1 del PREP), concluyendo el 7 de junio y deberá ser atestiguado preferentemente por un tercero con fe pública designado por el Instituto, conforme se señala en el inciso I del numeral 23, Capítulo I, Título III del Anexo 13 del Reglamento de Elecciones.

Entregables

Los productos para entregar, por parte del ente auditor, deberán incluir:

- Plan de trabajo detallado que cuente, como mínimo, con: el desglose de actividades, entregables, duración, fecha inicio, fecha fin y responsables de las actividades.
- Procedimiento técnico con el esquema de validación de los programas y de la base de datos del sistema informático previamente auditado del PREP, junto con las etapas de validación, generación de diagramas y descripciones correspondiente que se acuerden conjuntamente entre el Instituto y el ente auditor.
- Constancia de hechos de la generación de huellas criptográficas de los programas probados del sistema informático del PREP. Esta constancia deberá describir el protocolo de la actividad, fecha y lugar, hora de inicio y término, objetivo, actividades

realizadas, resultados obtenidos y las firmas autógrafas del personal participante por parte del Instituto y del ente auditor.

- Se deberá generar y almacenar bitácoras del sistema informático a fin de contar en todo momento con un respaldo de información que permita identificar los hallazgos y los ajustes realizados para la atención de estos. Lo anterior en conjunto entre el ente auditor y el Instituto.
- Constancias de hechos de la validación de los programas y de la base de datos del sistema informático del PREP. Estas validaciones se deberán realizar previo al inicio, durante y posterior al cierre de operaciones del PREP y deberán describir el protocolo de validación en el ambiente de producción del sistema informático del PREP. Además, deberán incluir la fecha y lugar, hora de inicio y término, objetivo, actividades realizadas, resultados y las firmas autógrafas del personal participante por parte del Instituto y el ente auditor.
- Informe de desempeño de la operación del sistema informático, de conformidad con el numeral 33, entregable número 25 del Anexo 13 del Reglamento de Elecciones del INE. Dicho documento deberá ser remitido de manera impresa dentro de los 30 días naturales posteriores a la jornada electoral.

Calendario de trabajo

El calendario de actividades para esta línea de trabajo deberá considerar que esta validación se lleva a cabo el día de la Jornada Electoral y al concluir la operación del PREP.

1.3 ANÁLISIS DE VULNERABILIDADES A LA INFRAESTRUCTURA TECNOLÓGICA

Objetivos

- Identificar debilidades de seguridad en la infraestructura tecnológica mediante la ejecución de pruebas de penetración y revisión de configuraciones de seguridad.
- Clasificar el impacto y documentar las vulnerabilidades identificadas con el propósito de recomendar al Instituto las posibles medidas para la mitigación de las vulnerabilidades que previamente fueron identificadas y documentadas.
- Verificar que las medidas implementadas por el Instituto se hayan atendido adecuadamente las vulnerabilidades reportadas.

Lo anterior conforme a lo establecido en el artículo 347, numeral 1, inciso b) del Reglamento de Elecciones.

Alcance

El análisis de vulnerabilidades de la infraestructura tecnológica deberá realizarse con base en las etapas que se describen a continuación.

I. Junta de inicio. Se convocará al personal involucrado en la realización de la auditoría con el objetivo de presentar las actividades consideradas como parte de la auditoría, definir los roles y responsabilidades de las partes, establecer las metodologías y estándares con las que se realizará la auditoría, así como los tiempos generales de ejecución.
   - El Instituto pondrá a consideración del ente Auditor una lista de activos durante la junta de inicio.
   - El Instituto proporcionará espacios de trabajo a los integrantes del ente auditor para que realicen el análisis de vulnerabilidades a la infraestructura tecnológica del sistema.
   - El Instituto otorgará los accesos correspondientes y las ventanas de tiempo necesarias para la ejecución de la auditoría.

II. Plan de trabajo detallado. Con base en la información obtenida y analizada, el ente auditor deberá elaborar el plan de trabajo en el que se incluyan los detalles del proyecto de auditoría de seguridad a la infraestructura tecnológica del PREP. Este documento integrará la información necesaria durante y después del proceso de auditoría e incluirá, como mínimo, lo siguiente:
   - Pruebas de penetración (pentest)
   - Revisión de configuraciones de seguridad

Pruebas de penetración (pentest)

Se deberán llevarán a cabo tanto desde el interior como desde el exterior de la red de datos a examinar y deberán enfocarse en:

- Servidores
- Aplicaciones web (se recomienda la metodología TOP 10 de OWASP)
- Equipos de telecomunicaciones

- Estaciones de trabajo
- Ataques a aplicaciones móviles (se recomienda la metodología OWASP Mobile Security Project)
- Pruebas de evasión de Firewalls y Web Application Firewalls (con técnicas tales como SQLMap, ModSecurity OWASP CRS, NMAP)

I. Presentación de hallazgos. El ente auditor deberá presentar un informe preliminar con los hallazgos encontrados, así como la recomendación para atender los mismos.

Para la presentación de hallazgos se utilizará un registro de datos en el que, de forma conjunta el ente auditor y el Instituto, puedan dar seguimiento a los mismos.

II. Validación de reporte de hallazgos. El Instituto presentará al ente auditor la retroalimentación acerca de los hallazgos encontrados con el fin de descartar falsos positivos (hallazgos que indican incorrectamente sobre la presencia de una vulnerabilidad) y homologar criterios de interpretación de dichos hallazgos.

III. Atención de hallazgos. Una vez validados los hallazgos, el Instituto aplicará los diferentes controles necesarios para mitigarlos y atenderlos. Cabe señalar que el ente auditor deberá considerar dentro de su plan de trabajo, otorgar al menos 10 días hábiles para que el Instituto pueda atender los hallazgos. Se deberá de calendarizar dichas actividades posterior al primer simulacro del PREP, para efectos de que la UCSI esté en posibilidades de solventar y atender los hallazgos que emita el ente auditor.

IV. Validación de la atención de los hallazgos. El ente auditor validará que el Instituto haya aplicado los controles necesarios para atender a los hallazgos reportados.

V. Entregables

El ente auditor deberá entregar los siguientes documentos derivados de la realización de pruebas de penetración (pentest):

Entregable	Descripción y Contenido	Criterios de Aceptación
Plan de pruebas de penetración a la infraestructura tecnológica	Describe los elementos generales de planeación que deben considerarse para el desarrollo de las pruebas de penetración. • Alcance • Calendario de trabajo • Responsables	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.

	técnicos	
Informe preliminar de las pruebas de penetración a la infraestructura tecnológica	Documento que contiene el resultado de las pruebas realizadas sobre los activos: • Resumen ejecutivo • Alcance • Resultado de las pruebas • Recomendaciones generales Para tener un mejor seguimiento de las incidencias que reporte el ente auditor, se deberá considera una herramienta automatizada que permita realizar la gestión de dichas incidencias, tal como MantisBT. El ente auditor podrá proponer otro software que cumpla con las funcionalidades de seguimiento a bugs e incidentes de software. Cabe señalar que dicha herramienta será auxiliar solamente, siendo el Informe preliminar el medio oficial del ente auditor para la remisión de los resultados de las pruebas realizadas. De igual forma, el Instituto deberá informarle al ente auditor respecto de la versión del sistema de la cual se está realizando la auditoría, para efectos de tener un mejor control sobre qué versión se está realizando la auditoría.	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.
Informe de la aplicación de recomendaciones de las pruebas de	Documento que describe el estado de seguridad de la infraestructura una vez que fueron aplicadas	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección

penetración a la infraestructura tecnológica	las recomendaciones por parte del ente auditor. • Resumen ejecutivo • Alcance • Resultado de la verificación	de descripción y contenido.
Informe de desempeño de la operación del sistema informático	Documento que describe el desempeño del sistema en términos de operatividad y funcionalidad. • Resumen ejecutivo • Alcance • Resultado de la verificación	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.

Revisión de configuraciones.

El objetivo es analizar las configuraciones de los dispositivos que conforman la infraestructura tecnológica con base en mejores prácticas de seguridad informática para identificar oportunidades y emitir recomendaciones orientadas al fortalecimiento de esta.

Entregables

Derivado de la revisión de configuraciones, el ente auditor deberá proporcionar al Instituto los siguientes documentos:

Entregable	Descripción y Contenido	Criterios de Aceptación
Plan de revisión de configuraciones de la infraestructura	Describe los elementos generales de planeación que deben considerarse para el desarrollo de la revisión: • Alcance • Calendario de trabajo • Responsables técnicos	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.

Informe preliminar de la revisión de configuraciones de la infraestructura	Documento que contiene el detalle de cada hallazgo identificado en la revisión de configuraciones. • Resumen ejecutivo • Objetivos • Alcance • Hallazgos y recomendaciones Para tener un mejor seguimiento de las incidencias que reporte el ente auditor, se deberá considera una herramienta automatizada que permita realizar la gestión de dichas incidencias, tal como MantisBT. El ente auditor podrá proponer otro software que cumpla con las funcionalidades de seguimiento a bugs e incidentes de software. Cabe señalar que dicha herramienta será auxiliar solamente, siendo el Informe preliminar el medio oficial del ente auditor para la remisión de los resultados de las pruebas realizadas. De igual forma, el Instituto deberá informarle al ente auditor respecto de la versión del sistema de la cual se está realizando la auditoría, para efectos de tener un mejor control sobre qué versión se está realizando la auditoría.	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.
Informe de la aplicación de recomendaciones de la revisión de	Documento que contiene el resultado final de la revisión de configuraciones: • Resumen ejecutivo	En formato electrónico. Contenido de acuerdo con los puntos señalados

configuraciones de la infraestructura	• Objetivos • Alcance	en la sección de descripción y contenido.

Informe final del análisis de vulnerabilidades

Al concluir las pruebas de penetración y revisión de configuraciones, el ente auditor deberá elaborar un informe final con el resultado del análisis de vulnerabilidades a la infraestructura tecnológica, de acuerdo con lo siguiente:

Producto	Descripción y Contenido	Criterios de Aceptación
Informe final del análisis de vulnerabilidades a la infraestructura tecnológica	Documento que contiene el resultado final del análisis de vulnerabilidades: • Introducción • Resultados Generales	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.

Calendario de trabajo

El calendario de actividades para esta línea de trabajo deberá establecer de forma clara los periodos de actividades, las fechas límite y los avances esperados.

1.4 PRUEBAS DE NEGACIÓN DE SERVICIO A SITIOS WEB DEL PREP Y AL SITIO PRINCIPAL DEL INSTITUTO

Objetivo

Realizar ataques de negación de servicio que permitan identificar, evaluar y aplicar las medidas necesarias para asegurar la correcta y continua disponibilidad del servicio Web de los sitios de publicación de resultados del PREP y del sitio oficial del Instituto, durante el periodo de operación del PREP. Se deberá documentar los hallazgos detectados durante la realización de las pruebas.

Alcance

Generar tráfico de red desde la infraestructura del ente auditor, o en su caso la que éste determine, hacia los servicios web del sitio de publicación del PREP, además del dominio del sitio oficial del Instituto.

Las pruebas de negación de servicio deberán considerar dos apartados:

- Tráfico no malintencionado que consiste en transacciones sintéticas que simulen el tráfico legítimo que se espera el día de la jornada.
- Tráfico de red malintencionado, consistente en paquetes de red malformados.

Las pruebas mencionadas anteriormente deberán realizarse de manera concurrente. Los ataques de negación de servicio deben contemplar, al menos, tráfico de red malintencionado con las siguientes características:

- Ataques volumétricos por protocolo TCP
    - Al menos de 400 Mbps de throughput
    - Al menos realizar SYN FLOOD
- Ataques volumétricos por protocolo UDP
    - Al menos de 400 Mbps de throughput
    - Al menos realizar DNS AMPLIFICATION
- Ataques volumétricos por protocolo ICMP
    - Al menos de 400 Mbps de throughput
    - Al menos realizar ICMP FLOOD
- Ataques en la capa de aplicación (HTTP)
    - Al menos realizar SLOWRIS ATACK

Las pruebas mencionadas anteriormente deberán realizarse de manera concurrente; considerando la generación de tráfico malintencionado (SYN FLOOD, DNS AMPLIFICATION, ICMP FLOOD, SLOWRIS ATACK) en un volumen que represente las condiciones de un ataque.

Durante las pruebas, cada simulación de ataque deberá apegarse a las condiciones de un ataque para hacer que el sitio web que se esté probando quede fuera de línea (no disponible) por, al menos 2 minutos, previo a que el Instituto efectué la contramedida para la mitigación.

Entregables

- Plan de trabajo detallado que cuente como mínimo con el desglose de actividades, entregables, duración, fecha inicio, fecha fin y responsables de las actividades.
- Plan de ataques de negación de servicio.
- Informe de resultados.
- Estadísticas del tráfico de red generado.

Calendario de trabajo.

El calendario de actividades para esta línea de trabajo deberá establecer de forma clara, los periodos de actividades, las fechas límite y los avances esperados.

CONDICIONES GENERALES

Por parte del ente auditor.

Para la realización de la auditoría, el ente auditor deberá presentar la siguiente documentación:

- Protocolos y metodologías de trabajo para llevar a cabo las actividades de cada auditoría definidas en los planes detallados de trabajo.
- Comprobar la experiencia de participación en proyectos similares, particularmente en las líneas de trabajo que forman parte de la presente auditoría.
- Presentar ejemplos de esquemas de validación de software, ejecutados en proyectos similares llevados a cabo anteriormente.
- El ente auditor deberá presentar ejemplos comprobables de informes relacionados con los resultados obtenidos en proyectos similares que haya realizado durante los tres últimos años.
- En su caso, carta de la máxima autoridad del ente auditor seleccionado, donde se acepte la colaboración con el Instituto para este proyecto.

Metodología para utilizar durante la auditoría informática del PREP 2021

La metodología para utilizarse por parte del ente auditor se deberá basar en la metodología de Hacking Ético, basado en el Top ten del Open Web Application Security Project (OWASP), para las siguientes etapas:

a) Footprinting
b) Fingerprinting
c) Escaneo de puertos
d) Análisis de vulnerabilidades
e) Pruebas de penetración basados en OWASP 2019 (pentest)

Respecto de los informes del ente auditor con las recomendaciones que en su momento proponga, podrán considerar lineamientos y/o referencias de entidades de seguridad reconocidas, tales como:

- Center for Internet Security (CIS)
- Open Web Application Security Project (OWASP)
- SANS Institute (SysAdmin Audit, Networking and Security)
- National Institute of Standards and Technology (NIST)
- Sitios oficiales de proveedores (Red Hat, Microsoft, Cisco, entre otros)

Para protección de la información generada por el ente auditor, y dentro del marco de normatividad aplicable del Instituto, la información que sea entregada por el ente auditor debe resguardarse con los mecanismos y procedimientos necesarios para evitar su divulgación a terceros.

Por parte del Instituto

Para la realización de las pruebas, el Instituto deberá proporcionar los siguientes insumos de información necesarios para la realización de las pruebas:

- Normatividad aplicable y vigente.
- Documentación técnica del sistema informático sobre la arquitectura tecnológica implementada (tanto de software como de hardware) y el proceso que se automatiza.
- Relación de los partidos políticos, coaliciones y candidatos independientes que participarán en la elección y su correspondencia con la geografía electoral aplicable a la elección.
- Ejemplares muestra de las actas de escrutinio y cómputo que se utilizarán en la elección.
- Base de datos con las casillas electorales aplicables a la elección.
- Capacitación inicial y apoyo técnico necesario.
- Usuarios y contraseñas respectivas para realizar las pruebas.
- Un ambiente de auditoría que permita controlar las versiones del Sistema Informático que se audite.

Durante el periodo de trabajo, el Instituto proporcionará al ente auditor, de todo lo necesario para la realización de las pruebas funcionales de caja negra, además de brindar la capacitación inicial y apoyo técnico necesario para habilitar la operación de esta.

Comunicación Social Conjunta

En el marco de trabajo se deberá considerar lo siguiente:

- Sesiones formales con periodicidad mensual para informar los avances de la auditoría y sesiones extraordinarias para atender cualquier situación de contingencia o riesgo.
- Comunicado público para informar la colaboración entre el ente auditor y el Instituto.
- Comunicado público para informar los resultados de la auditoría.