

Sistema de Cómputos Distritales y Municipales (SISCOM)

Proceso Local Electoral 2020-2021

Requisitos para la Auditoría Informática

INTRODUCCIÓN

El presente documento tiene como objetivo establecer los requisitos o elementos que el ente auditor designado para el SISCOM deberá de implementar, y con ello establecer áreas de oportunidad o mejora con el fin que el personal de la Unidad de Cómputo y Servicios Informáticos (UCSI) pueda agendar en el desarrollo del mencionado sistema.

Cabe señalar que los resultados de la auditoría serán analizados de igual forma por el Comité Técnico Asesor del SISCOM, para efectos de coadyuvar en el análisis de los mismos y en su momento establecer las recomendaciones pertinentes a la UCSI.

REQUISITOS ESTABLECIDOS EN LOS LINEAMIENTOS DEL SISCOM

De acuerdo con los Lineamientos del SISCOM, aprobados mediante acuerdo CG-0056-OCTUBRE-2017 de Consejo General del Instituto, en específico en su artículo 12:

1. *El Instituto deberá someter al SISCOM a una auditoría de verificación y análisis, para lo cual se deberá designar un ente auditor. Dicha auditoría deberá contemplar lo siguiente:*

a) *Pruebas funcionales de caja negra al sistema informático, para evaluar la integridad en el procesamiento de la información, la correcta transmisión y recepción de los datos y la generación de la base de datos de los cómputos.*

b) *Análisis de vulnerabilidades, considerando al menos pruebas de penetración y revisión de configuraciones a la infraestructura tecnológica del SISCOM.*

2. *Para la designación del ente auditor se dará preferencia a instituciones académicas o de investigación a nivel local y deberá efectuarse a más tardar, cuatro meses antes del día de la jornada electoral. El ente auditor deberá contar con experiencia en la aplicación de auditorías con los alcances establecidos en el numeral anterior.*

3. *Se deberá formalizar un instrumento jurídico en el cual se establezcan las cláusulas que el Instituto y el ente auditor, con el propósito de la realización de la mencionada auditoría.*

Dicho instrumento deberá contener como mínimo los siguientes elementos:

I. *Los alcances mínimos de la auditoría referidos en el presente artículo en su inciso 1;*

- II. *Metodología y plan de trabajo para realizar la auditoría, con calendario de actividades, responsables así como los recursos necesarios para llevarla a cabo;*
- III. *La información que por parte del Instituto pone a disposición del ente auditor, velando en todo momento por la protección de los derechos de propiedad intelectual;*
- IV. *Las obligaciones de las partes;*
- V. *La vigencia de dicho instrumento jurídico; y*
- VI. *La posibilidad de que el instrumento jurídico pueda modificarse siempre y cuando las partes estén de acuerdo y manifiesten su consentimiento por escrito.*
4. *El ente auditor deberá elaborar y entregar al Instituto informes de la auditoría:*
- I. Informe parcial: contendrá los resultados emitidos del proceso de auditoría, los cuales tendrán calidad de reservados en términos de las disposiciones aplicables en materia de transparencia y acceso a la información, incluyendo al menos, lo siguiente:*
- a) Los criterios utilizados para la auditoría;*
 - b) Los hallazgos identificados y clasificados, así como su método de clasificación;*
 - c) Las posibles recomendaciones que permitan al Instituto atender dichos hallazgos.*

ASPECTOS A CONSIDERAR EN LA AUDITORÍA DEL SISCOM

Con base en el punto anterior, la auditoría informática a realizarse del SISCOM, deberá contener por lo menos lo siguiente:

Pruebas funcionales de caja negra al SISCOM

El ente auditor deberá analizar el sistema informático del SISCOM, mediante la realización de pruebas funcionales de caja negra, para evaluar la integridad en el procesamiento de la información y generación de reportes. Deberá considerar, al menos, los siguientes aspectos:

- Analizar el funcionamiento de cada uno de los módulos operativos del SISCOM, incluyendo los siguientes: Administrador del Sistema, Jornada Electoral, Grupos de Trabajo (GT) y Puntos de recuento (PR), Captura de Cómputos, Reportes y aquellos módulos que en su caso se agregasen al SISCOM, previo al inicio de la auditoría respectiva.
- Se deberá realizar la captura de datos controlados (predefinidos) de 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. Los datos controlados contemplarán ciertos paquetes electorales con causales de recuento para efectos de validar la correcta funcionalidad de los módulos operativos del SISCOM, y posteriormente, una vez concluida la captura, se validará la generación de los reportes de cómputos oficiales.

Validación de las bases de datos del SISCOM

La base de datos que utilizará el SISCOM, deberá cumplir lo dispuesto respecto de la estructura de base de datos de cómputos establecida en el Anexo 15 y 18 del Reglamento de Elecciones.

Para ello, el Ente Auditor deberá revisar y validar la correcta generación de la base de datos con lo dispuesto en el mencionado Reglamento de Elecciones.

Análisis de vulnerabilidades a la infraestructura tecnológica

El ente auditor deberá realizar diversas pruebas en temas de seguridad informática, incluyendo:

- a) Pruebas de negación de servicio
- b) Inyección de código malicioso
- c) Pruebas de acceso a módulos del SISCOM

Se deberá utilizar metodologías o estándares a nivel internacional, tales como la **Guía de Pruebas OWASP**, o equivalentes.

ENTREGABLES POR PARTE DEL ENTE AUDITOR

Acorde a los Lineamientos del SISCOM además de lo establecido en el presente documento, el ente auditor deberá entregar, por lo menos, lo siguiente:

- Informe parcial de auditoría, que contendrá los resultados emitidos durante el proceso de auditoría, los cuales tendrán calidad de reservados en términos de las disposiciones aplicables en materia de transparencia y acceso a la información, incluyendo al menos, lo siguiente:
 - a) Los criterios utilizados para la auditoría;
 - b) Los hallazgos identificados y clasificados, así como su método de clasificación;
 - c) Las posibles recomendaciones que permitan al Instituto atender dichos hallazgos.
- Informe final de la auditoría, correspondiente a los resultados finales de la auditoría.

Ambos informes (tanto parcial como final), el ente auditor deberá entregar una versión ejecutiva (enfocado para revisión y análisis de los órganos directivos del Instituto) y una versión técnica, donde se realice una explicación más detallada respecto de cada una de las actividades y resultados generados por la auditoría informática del SISCOM.

ESTRUCTURA DE LA PROPUESTA

La propuesta que presente el ente auditor deberá estructurarse de la siguiente manera y deberá incluir, como mínimo, los siguientes aspectos:

- I. Propuesta técnica, respuesta a los rubros del presente documento.
- II. Propuesta económica.
- III. Plan de trabajo.
- IV. Presentación de metodología propuesta.
- V. Curriculum del ente auditor y su personal asignado (incluyendo en su caso, de cartas de referencia de trabajos de auditoría informática realizados con anterioridad).