REQUERIMIENTOS DE INFRAESTRUCTURA, SOPORTE Y LOGISTICA PARA LA OPERACIÓN DEL SOFTWARE DE ESCRUTINIO NACIONAL

Servicio para la actualización y mantenimiento del software de escrutinios, que utiliza el Consejo Nacional Electoral, para los procesos electorales a llevarse a cabo en las vigencias 2025 y 2026

Febrero 2026

INDRA COLOMBIA S.A.S.

Toda la información contenida en el presente documento y sus anexos tiene carácter confidencial, y sólo puede ser utilizada con el fin de ser evaluada por el destinatario (sea cliente, proveedor, colaborador, partners, etc.) de la misma y a los solos efectos de conducir los tratos comerciales, o de otra naturaleza, que motivan el envío del documento (en lo sucesivo, el "Propósito").

La información aquí presentada es propiedad de la Oferente que suscribe el presente documento, y es constitutiva de secreto empresarial (también denominado en determinadas jurisdicciones, secreto comercial), y además, puede estar protegida por derechos de autor, derechos afines, patente, modelo de utilidad y/o diseño industrial por lo que queda terminantemente prohibida su divulgación y/o transmisión a terceros sin el permiso previo, expreso y por escrito.

Se limitará al máximo el acceso a la información confidencial por parte del personal del destinatario de la misma, o del personal de aquellos terceros a los que se haya autorizado a acceder a la información confidencial, limitándose únicamente a aquellas personas cuyo acceso resulte estrictamente necesario, y debiendo el destinatario de la información confidencial garantizar que informa a dichas personas del carácter confidencial y propietario de la información así como del Propósito, asegurando que dicho personal trata la información confidencial única y exclusivamente para el Propósito, y absteniéndose de toda divulgación.

Una vez finalizado o concluido el Propósito, el cliente deberá restituir toda la información confidencial sin conservar ninguna copia de la misma, no pudiendo utilizarla de ninguna manera ni para ningún otro fin, salvo autorización previa, expresa y por escrito.

Copyright. Todos los derechos reservados. Colombia

Índice

1 Introducción 4

2 Arquitectura técnica del software 5

2.1 Arquitectura de las aplicaciones 5
2.1.1 Entorno en el que corre el software de escrutinio 7

2.2 Arquitectura de la base de datos 8

2.3 Arquitectura de la auditoría y trazabilidad de la aplicación 9

2.4 Arquitectura del Datacenter 11
2.4.1 Servidores Físicos 12
2.4.2 Máquinas virtuales 12

3 Requerimientos de Infraestructura 17

3.1 Infraestructura Tecnológica en la Comisión Escrutadora del CNE 17

3.2 Infraestructura Tecnológica para el Sistema WEB (Datacenter) 17

3.3 Hardware recomendado para el Datacenter 19

4 Requerimientos de Software Base 20

5 Requerimientos de Seguridad y respaldo de la información 21

5.1 Seguridad Informática 21

5.2 Características del Centro de Operaciones de Seguridad (SOC) 22

5.3 Requerimientos para el SOC (Security Operations Center) 23

5.4 Copias de Respaldo y Recuperación de la Información de la Infraestructura Tecnológica 24

6 Requerimientos de Soporte Técnico y Centro de Servicios TI 26

6.1 Soporte Técnico 26

6.2 Recurso humano especializado 28

1 Introducción

En este documento se describe el modelo de arquitectura técnica, donde se identifican los diferentes componentes que se deben ensamblar para que el código fuente del software de escrutinio nacional, pueda ejecutarse y operar adecuadamente en un entorno operativo que acompañe todo el proceso de la Comisión Escrutadora Nacional. Luego se detallan los componentes de infraestructura tecnológica requerida y se recomiendan más elementos para la implementación, operación y soporte del software de escrutinio de la Comisión Escrutadora Nacional del CNE para las elecciones de 2026.

2 Arquitectura técnica del software

2.1 Arquitectura de las aplicaciones

La solución se basa en un software centralizado, que debe ser desplegado en la infraestructura de un datacenter habilitado y disponible para la Comisión Escrutadora Nacional. La solución centralizada tiene las siguientes características:

- Control de la localización y la protección física de la ubicación del código fuente del Sistema de Escrutinio Nacional, reduciendo la exposición del mismo.
- Aprovechar la capacidad y rendimiento del HW instalado en el datacenter.
- Soluciones de contingencia robustas, con servidores en alta disponibilidad.
- Utilización de sistemas de autenticación centralizados, en alta disponibilidad, y blindados contra ataques externos.
- Despliegue y versionado del software centralizado de la Comisión.

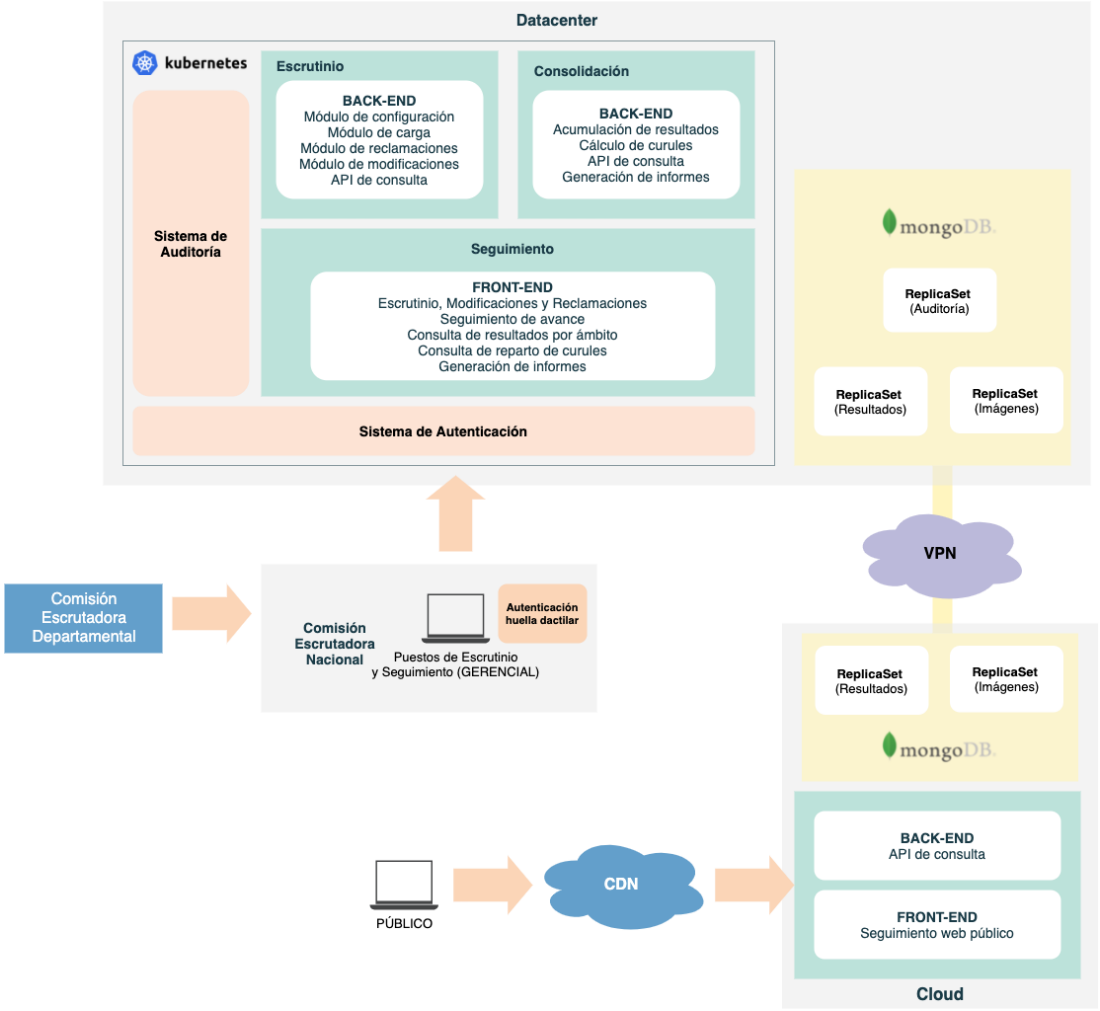
Para la configuración del escrutinio, se debe acceder a las aplicaciones desde estaciones de trabajo bastionadas y securizadas para este fin. Estos terminales se descargarán únicamente el frontend de las aplicaciones de Escrutinio General, que se comunicarán mediante conexión segura con los servidores, para realizar las operaciones necesarias de la comisión.

El único software requerido para la ejecución del Escrutinio General, que se encontraría fuera de la infraestructura del datacenter, sería el servicio de autenticación por huella dactilar de los miembros de la Comisión. Este servicio se ejecutará en los terminales utilizados por la comisión, y se comunicará de manera segura y protegida con las aplicaciones instaladas en el datacenter.

Los usuarios que quieran monitorear el proceso tendrán acceso por red privada a las aplicaciones de seguimiento web. En esta aplicación podrán visualizar el avance del Escrutinio General y el estado de las mesas.

Para los usuarios en internet, se dispondrá de una aplicación web en Cloud de acceso público, donde se podrá visualizar las imágenes de los E-24, E-26 y AGE de la Comisión Escrutadora Nacional, así como los E-14 de las mesas, por corporación.

A continuación, se presenta un diagrama de arquitectura del Sistema de la Comisión Escrutadora Nacional:



Las aplicaciones serán desplegadas sobre contenedores (docker) en un cluster de kubernetes. Para el desarrollo de las aplicaciones se utilizarán tecnologías de código abierto:

Servicios backend

Los servicios web son de tipo REST compatible con OpenAPIv3 y respuestas en formato tipo JSON. Como servidor de aplicaciones se utilizará Springboot, y lenguaje de programación JAVA mediante OpenJDK. Se implementan siguiendo el patrón de microservicios con Springboot, facilitando la abstracción, configuración y el escalado horizontal de cada uno de ellos.

Las APIs fueron diseñadas y documentadas mediante la herramienta open source Swagger, que permite la generación automática de código para diferentes lenguajes de programación. Los servicios del Sistema de la Comisión Nacional, implementan el API de OpenTracing para la generación de trazas distribuidas, que son recolectadas y visualizadas en el ELK del proyecto.

El acceso a los servicios de backend desplegados en el datacenter, debe ser securizado y autenticado por el Sistema de Autenticación del proyecto. Sólo se podría acceder a ellos desde el exterior del datacenter los equipos y usuarios autenticados, desde las aplicaciones web del Sistema de la Comisión Nacional.

Aplicaciones web Frontend

Las aplicaciones web del Sistema de la Comisión Nacional son desarrolladas mediante NodeJS y el framework frontend ReactJS.

Para el despliegue en los entornos de QA y Producción, se generan compilados de archivos estáticos (HTML, JS y CSS) con ofuscado de código, que son publicados mediante servidores Nginx. Estos archivos estáticos son descargados en las estaciones de trabajo bastionadas de la Comisión escrutadora para la realización del Escrutinio ya sea en modalidad sesión de comisión o consulta de los diferentes despachos y autoridades CNE y RNEC.

Las aplicaciones web utilizadas en el Escrutinio, se comunican con los servicios de Backend a través de la red interna del proyecto por un canal cifrado, y previa autenticación del equipo y del usuario que está operando el sistema.

Para los puestos de consulta del seguimiento web, a nivel gerencial, igualmente se realizará por la red interna del proyecto. Para la consulta pública, se debe dispondrá de una aplicación web en Cloud, que accederá de manera segura a la información del datacenter.

Sistema de Auditoría

Se implementa un servicio que permita recoger las auditorías realizadas en la Comisión Escrutadora Nacional. Existirán dos tipos de eventos, los que tengan que ver con la comisión, y los asociados a cada una de las mesas escrutadas. En ambos casos se formará un ciclo de auditorías encadenadas y protegida a cambios mediante un hash anidado, con tecnología blockchain, siguiendo el patrón de cadena de bloques..

Sistema de Autenticación

El acceso con privilegios a las aplicaciones del sistema, tanto para administradores, técnicos, operadores o todos los miembros de la comisión, será protegido mediante el Proveedor de identidades del proyecto.

En las estaciones de trabajo utilizadas por los miembros de la Comisión Escrutadora Nacional para la operación, se dispondrá de un lector de huellas, y un software embebido localmente, capaz de autenticar a los usuarios, y conceder privilegios en la utilización de las aplicaciones.

Servicios en Cloud (AWS Amazon)

Los servicios en Cloud se utilizarán para la publicación de información en internet, para el seguimiento del avance de la Comisión. Se dispondrá de unas bases de datos en replicación con las instancias del datacenter, de las que se obtendrán los datos únicamente de acceso público. Se desplegará una aplicación web con un API de consulta para este servicio.

2.1.1 Entorno en el que corre el software de escrutinio

El software actual de escrutinio nacional del CNE se encuentra desarrollado con el siguiente entorno tecnológico:

- MongoDB versión 5.0.7
- Java versión 11
- NodeJS versión 14

- Maven versión 3.8
- Keycloak versión 15.0.2
- AWS CLI versión v2
- API Gateway Kong versión 2.5.1
    - Percona PBM Agent versión 1.7.0

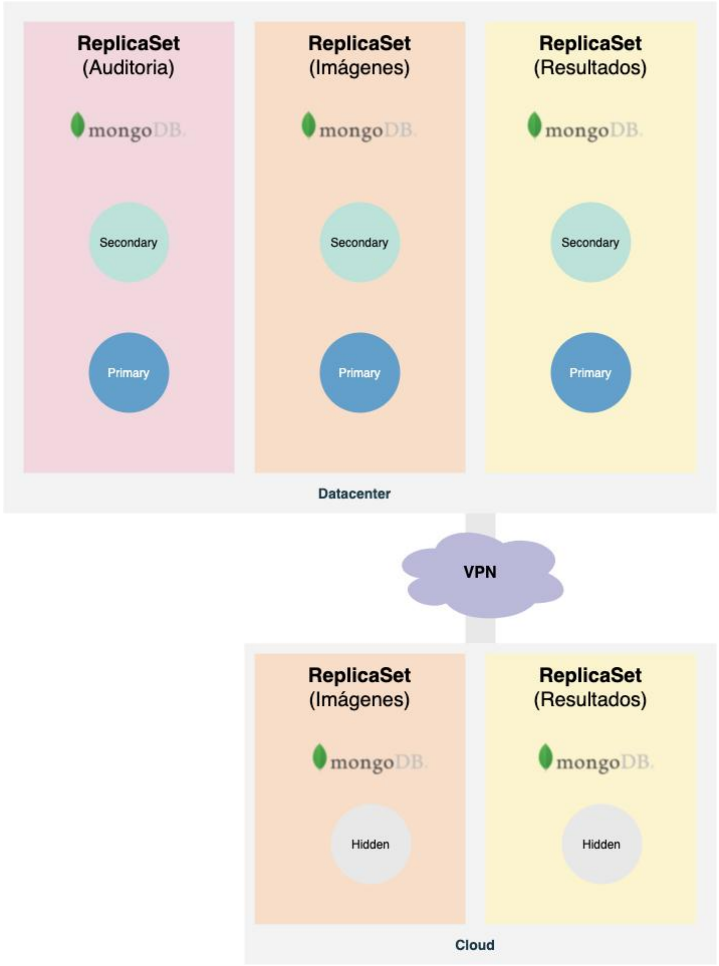
2.2 Arquitectura de la base de datos

Como motor de base de datos del Sistema de la Comisión Escrutadora Nacional, corre sobre el servidor de bases de datos NoSQL de tipo documental MongoDB, por los siguientes motivos:

- Tecnología **open source**, orientada al **BigData** capaz de almacenar y realizar operaciones sobre millones de registros, como por ejemplo los procedimientos de consolidación de resultados.
- Transacciones **ACID** (Atomicity, Consistency, Isolation, Durability) entre múltiples documentos, a partir de la versión 4.0 del motor.
- Formato **JSON**, lo que permite mantener la homogeneidad de modelo en las aplicaciones (frontend).
- Sencillez de construir arquitecturas escalables, mediante el **ReplicaSet**. Replicación asíncrona y diferentes tipos de instancias, que mejoran la Alta disponibilidad del Sistema:
    - **Primarias**, único miembro de la replicación capaz de escribir en las bases de datos.
    - **Secundarias**, útiles para el balanceo de operaciones de lectura y para el HA del ReplicaSet.
    - **Ocultas**, de sólo lectura, pero que no pueden ser elegidas Primarias hasta que se realicen cambios manuales en el ReplicaSet.

El replicaset de mongodb tiene un miembro primario que es elegido por votación entre todos los miembros de la réplica, en función del peso de cada uno. Si en un momento dado cayese la instancia primaria, se realiza una votación entre las instancias vivas y se elige un nuevo primario. Por eso, es necesario que la réplica disponga de un número impar de instancias, para que no se produzcan empates en el momento elegir al primario.

A continuación, se muestra el diagrama de arquitectura de la base de datos para el sistema de la Comisión Nacional.



Cada instancia de cada replicaset será desplegada sobre máquinas virtuales en el cluster de VMWare. Esta arquitectura contará con alta disponibilidad para el trabajo de la Comisión Escrutadora Nacional:

Primero, el HA propio de trabajar con el cluster de VMware. Si alguna de las instancias se cayera (por caída de un host de servidores), el VMWare automáticamente arranca el servidor en otro host.

Segundo, por el HA de la arquitectura de la base de datos, en el datacenter se dispone de más de una instancia de cada replicaset, por lo que, ante caída del primario, tomaría el control el secundario.

Ocultas, de sólo lectura, pero que no pueden ser elegidas Primarias hasta que se realicen cambios manuales en el ReplicaSet.

Se definen 3 tipos de ReplicaSet. Cada replicaset estará compuesto por un número de nodos, que garanticen la alta disponibilidad del sistema antes alguna contingencia. Además, cada uno de ellos contará con procedimientos de backups automático que respalden la información periódicamente, y se podrán ejecutar backups manuales desde la aplicación de Escrutinio.

2.3 Arquitectura de la auditoría y trazabilidad de la aplicación

Para el Sistema de la Comisión Escrutadora Nacional se programó un registro exhaustivo de los eventos que se realizan en el Escrutinio General, con el objetivo de contar con la trazabilidad de todas las

modificaciones que se realicen en los resultados, y de las operaciones realizadas durante el escrutinio. Para ello se desarrollará un servicio que recolectará las auditorías de manera horizontalmente en el proyecto.

La aplicación para recibir las **auditorías de la Comisión**, cuenta con las siguientes características técnicas:

- Desarrollando con la tecnología de Springboot, sobre imágenes de docker y desplegadas en el cluster de Kubernetes del datacenter, al igual que el resto de componentes software.
- Dispone de un servicio de balanceo de carga y los pods necesarios que garanticen el funcionamiento y la contingencia en el sistema.
- La persistencia de las auditorías se realiza sobre una instancia de Mongodb en un ReplicaSet de Auditoría independiente al resto del sistema.
- El servicio define un API REST mediante Swagger, con métodos de inserción y consulta de auditorías, nunca de modificación.
- El servicio requeriere autenticación mediante el gestor de identidades del proyecto.

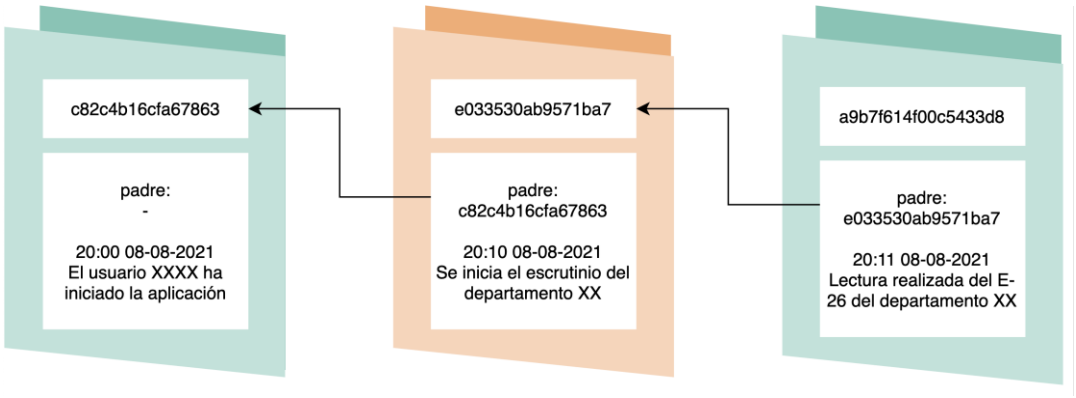
Este servicio recibie auditorías durante la operación de la Comisión, y se almacenarán siguiendo el patrón de diseño de **cadena de bloques**. Cada registro de auditoría es identificado con el cálculo de una función hash sobre el contenido de la entrada de auditoría. En el contenido de la auditoría se incluirá el hash del registro anterior de auditoría. La secuencia de hashes que une cada auditoría se remontará a la entrada de la mesa en el sistema.

Al incluir en el contenido de la auditoría la referencia al hash de la auditoría anterior, permite que, si alguna entrada de auditoría dentro del ciclo de vida es alterada, todas las referencias cambiarían en cascada, y se detectaría la vulnerabilidad.

El **contenido** de la auditoría, a partir del cual se obtendrá la referencia hash, será el siguiente:

- Referencia a la auditoría anterior.
- Timestamp de la creación de la auditoría.
- Tipo y descripción de la auditoría.
- Nuevo estado de la mesa o de la comisión.

Ejemplo de cadena de auditorías.



Se comprueba la integridad de la cadena de auditorías, verificando las referencias hash a las auditorías padre y verificando que los timestamp son incrementales. A través de la herramienta de Seguimiento web, se podrá visualizar el ciclo de vida de la comisión y de cada mesa.

2.4 Arquitectura del Datacenter

En este punto se describen los lineamientos tecnológicos recomendados para el CPD o Datacenter, como son los servidores, físicos y virtuales y el almacenamiento que constituyen la infraestructura electoral. Por otro lado, se incluyen las especificaciones del CPD propuesto donde se alojará el equipamiento.

El equipamiento debe ser suministrado por empresas líderes del mercado tecnológico que garantizan el mantenimiento del equipamiento hardware, como servidores, cabinas de discos y electrónica de red, asegurando su calidad y puesta a punto durante todas las fases del proyecto. Los principios que se aplican en el diseño de esta arquitectura son los siguientes:

Escalabilidad: La solución propuesta agrupa los recursos de tal forma que se proporciona escalado horizontal, sin pérdida de servicio, de cada capa (Microservicios, BBDD, seguridad, etc. De esta manera, la infraestructura puede ampliarse gradualmente en el caso de que sea necesario tras las correspondientes pruebas de carga y optimización.

Este crecimiento lineal y predecible de la capacidad y del rendimiento es uno de elementos esenciales de la arquitectura.

Rendimiento: Para obtener el máximo rendimiento es necesario asignar dinámicamente los recursos como la CPU, la memoria, el ancho de banda y la capacidad de almacenamiento según se requiera por cada aplicación. Para ello se necesita desagregar los servidores de su carga de trabajo virtual.

La desagregación significa separar de los servidores físicos cada uno de sus recursos de CPU, memoria, etc. para que estos puedan asignarse globalmente en un clúster según sea necesario y de acuerdo con las necesidades de la carga de trabajo de cada aplicación. Esto se realiza mediante la virtualización de los recursos físicos de cada servidor como la CPU, la memoria, el ancho de banda y el almacenamiento, poniéndolos al servicio de una arquitectura virtual.

Flexibilidad: En cuanto a la flexibilidad, la solución de arquitectura virtual propuesta presenta, entre otras ventajas, la facilidad y rapidez para migrar una aplicación ejecutada en un entorno virtual hacia un nuevo servidor físico.

Alta disponibilidad: La alta disponibilidad ofrece una protección contra fallas del hardware o del sistema operativo. Las máquinas virtuales y los servidores físicos son monitorizados constantemente para detectar posibles fallos, ocasionando que se reinicien las máquinas virtuales en otros servidores físicos sin intervención manual cuando se detecte un problema.

Seguridad: La seguridad de la arquitectura se fundamenta en dos principios, el de conceder el mínimo privilegio, limitando el alcance de acceso que un usuario o proceso tiene en el sistema y a qué datos puede acceder.

Virtualización: Mediante la virtualización del hardware, es posible ejecutar múltiples sistemas operativos o máquinas virtuales en un mismo servidor físico. Esta tecnología de virtualización implica la separación del hardware físico en máquinas virtuales donde se emula, en cada una de ellas, el hardware de una máquina física.

Tiene como ventajas más significativas que se reduce la cantidad de servidores físicos que se deben instalar, además de facilitar el mantenimiento del hardware, y con el consiguiente ahorro de espacio y de consumo de energía.

Adicionalmente a esta división en capas, desde la capa física a la virtual, se agrega otra capa de gestión de las aplicaciones, la configuración de un clúster Kubernetes on-premise.

La Infraestructura de virtualización incluye los siguientes componentes:

Servidores Proxmox: Hipervisor de tipo 1 que se ejecuta en servidores físicos y que virtualizan la CPU, la memoria RAM, los discos y las redes para crear múltiples máquinas virtuales en una máquina física.

Máquinas virtuales donde se instalan Sistemas Operativos completos sobre una estructura virtualizada de CPU, RAM, disco y red. El tipo de máquinas virtuales que se instalan incluye desde los nodos de Kubernetes (Plano de Control y de Datos), servidores de monitoreo, firewall y el resto del clúster de Vmware 6.x.

Clúster Kubernetes. Es una plataforma de orquestación de contenedores de código abierto diseñada para automatizar la implementación, el escalado y la administración de aplicaciones en contenedores.

Red Interna virtualizada compuesta de switches virtuales para interconectar las máquinas virtuales entre sí y con los switches físicos a través de las tarjetas de red de los servidores.

Electrónica de Comunicaciones que comunican el mundo virtual con el mundo físico. Compuesto de switches de comunicaciones y routers principalmente.

Almacenamiento compuesto por los discos físicos donde se instalan las máquinas virtuales que se reparten por todos los nodos del clúster virtual.

2.4.1 Servidores Físicos

El clúster virtual se forma a partir de un número de servidores físicos con tecnología x86 superior y donde se ejecuta un hipervisor de tipo 1 en cada uno de ellos. Todos los servidores se configuran de igual manera y tienen características hardware similares (CPU, memoria, discos locales) por lo que son vistos por el clúster como nodos equivalentes de ejecución. Cada servidor ejecuta de forma independiente la carga de máquinas virtuales que le haya sido asignada. Sobre el clúster de servidores físicos se ejecutan las máquinas virtuales sobre las cuales, a su vez, se instala el clúster de Kubernetes, con los namespaces de cada uno de los ambientes de producción, QA, desarrollo y capacitación si fuera necesario.

El clúster se compone de un grupo de servidores físicos y máquinas virtuales. Ambos tienen acceso a los recursos compartidos del clúster, como las redes de comunicaciones internas, comunicaciones externas y elementos de almacenamiento. Todos los elementos se administran de forma centralizada y conjunta desde una herramienta única de configuración (Proxmox).

En principio, cualquier máquina virtual podría ejecutarse de forma automática en cualquier servidor físico. Sin embargo, si esto fuera así, podría darse el caso de que el reparto de carga automático entre los servidores llevara a una situación donde máquinas virtuales con mayores necesidades de recursos se encontraran ejecutándose en el mismo servidor, lo que podría llevar a una pérdida de rendimiento de alguno de los servicios.

Para obtener el mejor balanceo de carga entre los servidores y hacer el mejor uso posible de los recursos de CPU y memoria de todos los hipervisores, se opta alternativamente por una configuración manual de asignación de recursos, donde se fijan de antemano en qué servidor se puede ejecutar cada máquina virtual.

El rack estará destinado únicamente al sistema electoral del escrutinio general, no compartiendo capacidades con otros sistemas o procesos electorales.

2.4.2 Máquinas virtuales

El clúster de Proxmox se compone de máquinas virtuales (MV). La asignación de máquinas virtuales a servidores físicos se basa en reglas preestablecidas para obtener el mayor rendimiento y alta

disponibilidad. Como se ha indicado anteriormente, la asignación se hace manualmente aplicando reglas de afinidad que permiten distribuir un grupo de máquinas virtuales en diferentes hosts Proxmox o mantener un grupo de máquinas virtuales en un host Proxmox en particular.

Una regla de afinidad coloca un grupo de máquinas virtuales en un servidor Proxmox o grupo de servidores Proxmox para garantizar los recursos y el rendimiento de estas máquinas virtuales. Una regla de anti-afinidad, por el contrario, coloca un grupo de máquinas virtuales en diferentes nodos, lo que evita que todas las máquinas virtuales fallen a la vez en caso de que falle un nodo, con lo que se obtiene alta disponibilidad en el servicio que proporcionan. Las reglas de afinidad y anti-afinidad pueden ser de uso obligatorio o deseables:

- Regla obligatoria. Si no se pueden cumplir las reglas de afinidad o anti-afinidad, las máquinas virtuales incluidas en este tipo de reglas no se pueden arrancar. Como ejemplo, establecer que una determinada máquina virtual solo se pueda arrancar en un conjunto de servidores Proxmox, creando de esta manera unidades o conjuntos de ejecución más pequeños que el clúster en su totalidad.
- Regla deseable. Si no se pueden cumplir este tipo de reglas de afinidad o anti-afinidad, las máquinas aún se pueden arrancar. Es decir, es una condición deseable que se cumpla la regla, pero su incumplimiento todavía permite que se dé el servicio, aunque quizá con menor rendimiento del esperado. Como ejemplo, que dos máquinas virtuales relacionadas compartan un nodo físico y disminuir de esta forma los retardos de comunicaciones entre ellas al encontrarse en el mismo servidor físico Proxmox.

La elección y ajuste de las reglas se realiza mediante una estimación inicial, pero su definición final en producción queda sujeta a las pruebas de carga y rendimiento que se consideren posteriormente. Para obtener el máximo rendimiento, se han agrupado las máquinas virtuales relacionadas de tal forma que se optimiza el tiempo de acceso entre máquinas virtuales relacionadas, al producirse la comunicación dentro de la misma máquina y evitándose los retardos de red si las máquinas virtuales se encontraran repartidas entre varias máquinas físicas.

Notar, sin embargo, que esto no significa que la alta disponibilidad se vea disminuida, ya que, en el caso de caída de la máquina física, sus máquinas virtuales migrarían automáticamente a otra u otras máquinas físicas para continuar ofreciendo el servicio.

Se continúa con una descripción de los elementos que son los encargados de servir las aplicaciones que forman parte del proceso de escrutinio nacional.

Clúster de Kubernetes

Los servicios que implementa el Sistema Electoral se ejecutan en máquinas virtuales y en contenedores. Para orquestar la ejecución de estos contenedores se necesita un software especializado como es Kubernetes. Kubernetes es un marco de orquestación de contenedores que, en la aplicación de escrutinio, son de tipo Docker. Estos contenedores se alojan en una versión de Kubernetes que se ejecuta on-premise e instalado sobre máquinas virtuales.

El uso de Kubernetes facilita la gestión de los contenedores en su conjunto, facilitando, por ejemplo, el escalado y el despliegue, adecuándose además a los requerimientos de rendimiento exigidos por las necesidades del Proceso Electoral y al mismo tiempo garantizando la utilización eficiente de los recursos como son la CPU y la memoria RAM de la infraestructura existente.

El clúster está formado por tres nodos maestros donde se ejecuta la API, mientras que en el resto de los nodos (workers) se ejecutan los Servicios electorales mediante contenedores Docker.

Balanceadores

El balanceo de carga del clúster de kubernetes se realiza mediante 2 balanceadores Haproxy y el servicio keepalived. El servicio keepalived permite compartir una IP entre ambos balanceadores Haproxy, creando una configuración activo/pasivo con conmutación automática del servicio.

Servidores Mongo

Como motor de base de datos del Sistema Electoral se eligió MongoDB, por los siguientes motivos:

- Tecnología open source, orientada al BigData capaz de almacenar y realizar operaciones sobre millones de registros, como por ejemplo los procedimientos de acumulación del Sistema de Totalización sobre el total de las mesas y elecciones.
- Transacciones ACID (Atomicity, Consistency, Isolation, Durability) entre múltiples documentos, a partir de la versión 4.0 del motor.
- Formato JSON, lo que permite mantener la homogeneidad de modelo en las aplicaciones.
- Sencillez de construir arquitecturas escalables, mediante el ReplicaSet. Replicación asíncrona y diferentes tipos de instancias:
    - Primarias, único miembro de la replicación capaz de escribir en las bases de datos.
    - Secundarias, útiles para el balanceo de operaciones de lectura, y para el HA del ReplicaSet.
- El replicaset de mongodb tiene un miembro primario que es elegido por votación entre todos los miembros de la réplica, en función del peso de cada uno. Sí en un momento dado cayese la instancia primaria, se realiza una votación entre las instancias vivas y se elige un nuevo primario.
- Por eso, es necesario que la réplica disponga de un número impar de instancias, para que no se produzcan empates en el momento elegir al primario.

Zabbix

Mediante la herramienta Zabbix, de código abierto, se tiene un conocimiento en tiempo real del estado de toda la infraestructura, identificando los eventos que causan problemas y así favorecer la manera de resolverlos de forma efectiva. Los elementos que se monitorizan son la CPU, memoria RAM, espacio consumido de disco y tráfico de red de cada uno de los componentes que constituyen la infraestructura.

ELK

El sistema de registro y auditoría de eventos que implantará Indra estará basado en el stack ELK (ElasticSearch-Logstash-Kibana) de código abierto. ElasticSearch es un motor de búsqueda de para todo tipo de datos. Los datos fluyen hacía Elasticsearch desde distintas fuentes de datos, logs, métricas de sistema y aplicaciones web siendo almacenados en formato JSON distribuidos en diferentes índices. Logstash se usa para el procesamiento de datos realizando la ingesta de datos en los índices de ElasticSearch con un parseo enfocado a su mejor procesamiento, ayuda a diferenciar los datos numéricos, de texto, geoespaciales, etc. Kibana es el interfaz web que ayuda a la consulta y visualización de todos los datos almacenados de una manera simple e intuitiva, permitiendo la generación de tableros personalizados para cada sistema y/o aplicación.

Los eventos pueden ser enviados al SOC para su análisis con una herramienta SIEM, la instalación de esta herramienta es para uso interno ya que facilita el estudio de los componentes durante su uso.

El stack de ELK es conocido por la centralización de logs. Se apoya en Elasticsearch, como motor de búsqueda, el cual proporciona una búsqueda eficiente de texto completo y capacidades de filtrado

simples. Este almacén permite almacenar datos extraídos de logs parseados con la ayuda de logstash, tanto de texto como numéricos.

Con el uso de los diferentes agentes de datos, el stack facilita la recopilación de todo tipo de datos. Mediante MetricBeat, el agente de datos específico para las métricas, añadimos un pilar más para la correlación de datos de manera integrada. Es totalmente compatible con las métricas de Kubernetes, y su despliegue en la plataforma es integrable también con Prometheus. De esta manera podremos conocer de manera detallada los consumos de los diferentes contenedores desplegados en la plataforma.

Por otro lado, la monitorización de la plataforma se ayudará de APM, que es un sistema de monitoreo de rendimiento de aplicaciones compatible con Opentracing. Nos facilita la monitorización de software y aplicaciones en tiempo real, como son los tiempos de respuesta en solicitudes HTTP entrantes o salientes, los tiempos de las consultas en bases de datos, etc. Incluyendo el rastreo distribuido, podremos conocer el tiempo completo de las transacciones a su paso por los diferentes componentes (servicios o microservicios). APM requiere de unos servidores APM, que están instalados dentro de los nodos de ELK y unos agentes en las aplicaciones. Los agentes son aptos para los lenguajes que se usarán en el proyecto, Java y Node.js.

SAA

El Sistema de Autenticación y Autorización está formado por un servidor FreeIPA y otro servidor KeyCloak.

El servidor FreeIPA, servidor de administración de identidad (IDM), proporciona un servicio integrado de autenticación y autorización que combinando diversas tecnologías de código abierto permite un único punto de autenticación. Las tecnologías que utiliza son las siguientes:

- Servicio de Directorio donde los usuarios y grupos se asignan con identificadores y es donde se realiza en definitiva la gestión de identidades, asignando usuarios a grupos y estos a roles a los específicos.
- Kerberos Proporciona servicios de autenticación para todo el ámbito o dominios de FreeIPA, como es el servicio de usuario. El servidor Kerberos es uno de los componentes principales servidor FreeIPA.
- LDAP Basado en OpenLDAP, permite acceder a los datos almacenados del servidor FreeIPA , desde los clientes que soporten este protocolo, lo que le concede a FreeIPA la posibilidad de ser accedido desde cualquier cliente que soporte autenticación por medio de LDAP
- Servidor NTP, servidor para la sincronización de hora de todos los componentes del sistema conectado a un servidor externo stratum 2.
- Servidor DNS, resuelve los nombres de los dominios configurados en el sistema.
- PKI, ofrece la gestión de certificados y claves del sistema.

Este sistema centraliza la autenticación y autorización de los usuarios, grupos, máquinas y en general todos los objetos involucrados en el Proceso Electoral.

Junto a Keycloak, que es un proyecto de código abierto, se proporciona gestión de identidad y acceso para las aplicaciones electorales. Keycloak también se integra con el servicio SSSD (System Security Services Daemon).

Las características principales de Keycloak son las siguientes:

- Single-sign on (SSO) Inicio de sesión único que permite a las aplicaciones (usuarios) cliente autenticarse contra Keycloak en lugar de cada aplicación o servicio individual. Una vez que los

usuarios inician sesión en Keycloak, pueden acceder a cualquier aplicación o servicio que esté autenticado a través de Keycloak.

- Federación de usuarios Permite que las autenticaciones se hagan en un servicio externo dispuesto a tal fin, como FreeIPA, además de autenticar con una base de datos local se pueden federar fácilmente con Keycloak.
- Protocolos estándar Keycloak, listo para usar, brinda soporte para OpenID Connect, OAuth 2.0 y Security Assertion Markup Language (SAML).

3 Requerimientos de Infraestructura

A continuación, se detallan los requerimientos recomendados para la correcta implementación del software de escrutinio nacional.

3.1 Infraestructura Tecnológica en la Comisión Escrutadora del CNE

Para el montaje físico del sistema en la que se defina como sala de audiencia y despachos de los diferentes comisionados/magistrados del CNE, se recomiendan los siguientes equipos:

- Once (11) Computadores portátiles para la Audiencia Pública de Escrutinios.
- Dos (02) Computadores portátiles por cada uno de los Despachos de los diez (10) Magistrados del CNE y dos (2) más para la Secretaría de la comisión escrutadora nacional a cargo del Registrador Nacional del Estado Civil.
- Un (1) Impresora láser y su backup, que garanticen los niveles de calidad y velocidad necesarios para el proceso, la cual deberá tener papel y tóner suficientes para cubrir la totalidad de impresiones requeridas por la Comisión Escrutadora Nacional.
- Un (1) escáner y su backup, para la impresión y digitalización de las actas E-24 Y E-26, Acta General de escrutinio y demás documentos para cuando la Comisión Escrutadora Nacional se encuentre en sesión.
- Diez (10) lectores de huella que operen bajo formato ISO, para cada la comisión escrutadora, más un (1) lector de backup.
- Diez (10) computadores y diez (10) escáneres para la digitalización de las reclamaciones recibidas.
- Tres (03) pantallas para visualizar el avance de la Comisión Escrutadora Nacional mientras se encuentre en sesión.
- Se deberá facilitar en la Comisión Escrutadora, el suministro de multi tomas y extensiones eléctricas, cuando se requieran.
- Se deberá disponer para la Comisión Nacional los medios de comunicación para acceder al sistema de Escrutinio en una red privada. De igual manera, los elementos técnicos para lograr dicha instalación garantizando un canal principal y uno de contingencia.

3.2 Infraestructura Tecnológica para el Sistema WEB (Datacenter)

La solución deberá incluir servidores físicos y/o virtuales que garanticen las siguientes características:

- Alta disponibilidad de los servidores.
- Tolerante a fallas físicas y/o de datos.
- Medios de comunicación redundantes.
- Hardware y/o software para balanceo de carga web.

- Se debe proveer de capacidades de Procesamiento, Memoria y CPU, según las capacidades (para una disponibilidad de 99,6%) y licenciamiento en las capas de Sistema Operativo, Base de Datos y Servidores de Aplicaciones.

- Se debe proveer una capacidad de almacenamiento suficiente para mantener los procesos de Congreso, Presidente, de manera concurrente.

- Se deben prestar todos los servicios de tecnología requeridos en un datacenter que cuente con certificación TIER III, y/o ICREA IV y/o superior y debe estar en la capacidad de prestar los mismos servicios bajo la modalidad de Nube Privada. Entiéndase nube privada como el aprovisionamiento de un conjunto de recursos físicos y/o virtuales que No puede ser compartida de manera física con otros clientes, y lógicamente debe estar configurada y monitoreada de manera independiente para la Entidad.

- Los recursos que están alrededor de la infraestructura física del datacenter como redes, energía, refrigeración, seguridad física, entre otros, pueden ser compartidos. Las configuraciones iniciales y las modificaciones de los servicios estarán a cargo del implementador como parte de la administración de la plataforma y requerimientos propios de la Entidad.

- El alojamiento de toda la infraestructura física en el datacenter debe estar en uno o más racks 100% dedicados y exclusivos para la solución informática de software de escrutinio nacional, asegurando la disponibilidad en potencia de energía y comunicaciones necesaria para la operación del sistema.

- Se debe garantizar el soporte de fábrica vigente de todo el licenciamiento de las plataformas base de software y/o hardware que soportan los servicios de tecnología del software de escrutinio nacional, esto durante la operación en producción del sistema.

- Se debe mantener las plataformas actualizadas a las últimas versiones y parchadas con el fin de atender la gestión de vulnerabilidades del proceso de gestión de seguridad de la información de la Entidad.

- El proveedor del servicio y los fabricantes atenderán cualquier anomalía que se presente en los equipos, o en su defecto, proceder a reemplazarlos por otros de iguales o superiores características. Para atender cualquier evento que se presente en los equipos o para proceder a reemplazarlos, se requerirá un protocolo de reemplazo acordado con la Entidad, el cual deberá contener la autorización para ejecutar el procedimiento.

- Se debe Disponer de un (1) procedimiento documentado para atender cualquier eventualidad o contingencia, que impida la normal operación del proceso electrónico de los escrutinios, entendiéndose como contingencias aquellos problemas técnicos o impedimentos relacionados con software, hardware o comunicaciones.

- Garantizar en el Data Center para el Sistema de Seguimiento y Control en la WEB de los escrutinios las redundancias requeridas en materia de hardware, comunicaciones y electricidad.

3.3 Hardware recomendado para el Datacenter

Para la implementación del ambiente productivo principal, se recomiendan las siguientes características de infraestructura central, todas instaladas de manera dedicada y en racks de uso exclusivo de la solución de Escrutinio Nacional:

Switching - Networking:

- 2 switches de 48 puertos cada uno.
- Conectividad: 25 GbE.

Servidores de procesamiento y almacenamiento

(total: **8 unidades**). Cada servidor debe contar con:

- 2 procesadores Intel Xeon Platinum 8452Y.
- 512 GB de RAM.
- 4 TB de almacenamiento SSD.
- 6 puertos de red de 25 GbE.

4 Requerimientos de Software Base

Se requiere del siguiente software base descrito en el entorno de la aplicación, para que se pueda instalar y ejecutar correctamente todos los módulos y componentes del software de escrutinio nacional:

Solución biométrica:

- Neurotechnology SDK 2025.1.
- Debe incluir los siguientes módulos adicionales:
  - 12 × FingerPrint Client.
  - 12 × FingerPrint Matcher.

Base de datos:

- MongoDB Community Edition 8.

Contenedores:

- Kubernetes versión 1.34 o superior
- Registry (repositorio de contenedores).

API Gateway:

- API Gateway compatible con APISIX o equivalente.
- Debe soportar configuración OIDC (OpenID Connect).

Gestión de identidades:

- Keycloak versión 26.4 o superior

Servicios internos:

- Servidor DNS interno.
- Servidor NFS (o sistema equivalente) para compartir ficheros entre pods dentro del clúster.

5 Requerimientos de Seguridad y respaldo de la información

5.1 Seguridad Informática

Además de implementar sus propios procedimientos y solución de ciberseguridad, el implementador deberá cumplir con las políticas específicas de seguridad de la información y los lineamientos establecidos por la Entidad, así como respetar estrictamente los acuerdos de confidencialidad suscritos.

Para la solución integral del software de escrutinio en producción, se debe implementar, mantener y garantizar el correcto funcionamiento de las siguientes plataformas tecnológicas como parte integral del servicio de seguridad informática:

- Firewalls de última generación.
- Sistemas de contención y mitigación de ataques DDoS.
- Soluciones de detección de malware de día cero (día-0).
- Soluciones de protección de endpoint con antivirus actualizados.

- Se debe asegurar la protección integral de la plataforma tecnológica que soporta el software de escrutinio utilizado por el Consejo Nacional Electoral (CNE), incluyendo la instalación, configuración, administración y monitoreo continuo de todos los componentes tecnológicos involucrados.

- Se debe garantizar la trazabilidad completa de la información y los eventos de seguridad, implementando las medidas necesarias para la identificación, mitigación y gestión oportuna de amenazas y riesgos informáticos que puedan afectar la integridad, disponibilidad o confidencialidad de la información de la Entidad.

- Implementar un mecanismo de doble factor de autenticación (2FA) para el acceso al sistema de escrutinio a cargo del CNE, conforme a los estándares y políticas de seguridad definidos por la Entidad, con el fin de fortalecer la protección del sistema contra accesos no autorizados.

- Garantizar el tráfico de información en forma segura y confiable dentro de la red de comunicaciones, empleando para ello las herramientas de hardware y software necesarias para optimizar la seguridad informática de los datos e impedir cualquier posibilidad de

5.2 Características del Centro de Operaciones de Seguridad (SOC)

Es indispensable acompañar la solución con un servicio integral de Centro de Operaciones de Seguridad (SOC), que permita anticipar, detectar, gestionar y responder de forma proactiva a cualquier situación que pueda comprometer la seguridad de los servicios tecnológicos asociados a dicha solución informática, para lo cual se compromete a:

1. Garantizar un servicio de monitoreo continuo bajo el esquema 7x24 durante los procesos de escrutinio de Congreso y Presidente 2026, con recurso humano especializado ubicado en las instalaciones del proveedor, enfocado en la gestión de eventos e incidentes de seguridad en servidores, redes, dispositivos, bases de datos y demás componentes que soportan el funcionamiento del software de escrutinio nacional.

2. Notificar de forma inmediata cualquier evento de seguridad detectado a los especialistas del centro de servicios y a la Entidad, a fin de facilitar la atención, investigación y toma de decisiones correspondiente.

3. Proveer las herramientas, plataformas e infraestructura tecnológica necesarias para la adecuada prestación del servicio SOC, las cuales deberán ser licenciadas. Queda expresamente prohibido el uso de software libre para este propósito.

4. Implementar recursos, procesos y tecnologías que apoyen la identificación, análisis, gestión, respuesta y seguimiento de incidentes de seguridad sobre los activos tecnológicos involucrados en la solución informática de escrutinio nacional, incluyendo: servidores, aplicaciones, seguridad perimetral, redes, comunicaciones, entre otros.

5. Garantizar que la comunicación de logs entre la Entidad y el SOC del sistema de escrutinio se realice a través de canales seguros, sin causar degradación o afectación del servicio.

6. Medir y monitorear la disponibilidad de los activos tecnológicos involucrados en el servicio de correlación, generando alertas en caso de interrupciones o degradaciones del servicio.

7. Asegurar que la infraestructura tecnológica asociada al SOC cuente con mecanismos de separación física y lógica, que garanticen la confidencialidad e integridad de la información procesada.

8. Registrar todos los requerimientos, eventos e incidentes a través de la herramienta de gestión ITSM establecida por la Entidad.

9. Contar con un proceso formal de gestión de incidentes de seguridad, que incluya desde la detección inicial hasta la contención, investigación y resolución. Este proceso deberá contar con personal técnico idóneo y certificado, que participe activamente en la gestión de cada incidente.

10. Realizar la correlación de eventos de seguridad, incluyendo actividades de captura, integración, análisis, generación de alertas, informes y retroalimentación. La solución deberá permitir la gestión y monitoreo continuo de la seguridad de la infraestructura y usuarios.

11. Mantener la información correlacionada durante un periodo mínimo de un (1) mes, asegurando su disponibilidad para consulta y análisis.

12. Prestar el servicio de correlación de eventos mediante una plataforma SIEM, capaz de consolidar logs y eventos de seguridad provenientes de diferentes plataformas mediante políticas predefinidas (casos de uso). Esta plataforma deberá:

    - Identificar, alertar, gestionar y correlacionar eventos que comprometan la confidencialidad, integridad o disponibilidad de los activos tecnológicos de la Entidad.
    - Detectar, responder y neutralizar amenazas mediante la recolección centralizada de eventos y alertas de seguridad.
    - Estar soportada por una solución que acepte al menos los siguientes mecanismos de recolección de eventos/logs: Syslog; WMI; FTP/SFTP; Database; OPSEC; CEF

13. Proveer una solución SIEM alimentada por fuentes de inteligencia de amenazas, que incluya listas de reputación y/o dominios sospechosos, permitiendo la verificación de indicadores de compromiso.

14. Acreditarse como proveedor autorizado del fabricante de la solución SIEM utilizada, para garantizar que cumple con los estándares técnicos exigidos.

15. Ejecutar de manera continua el monitoreo y verificación de logs y alarmas, realizando análisis preventivos que permitan generar planes de acción y efectuar el seguimiento a los aspectos relacionados con la calidad del servicio.

5.3 Requerimientos para el SOC (Security Operations Center)

1) Facilitar un centro de operaciones de seguridad (SOC) que garantice la anticipación de incidentes de seguridad, el análisis permanente de riesgos y la detección temprana de amenazas contra los activos de información de la Entidad.

2) Identificar, analizar y contener posibles ataques a la infraestructura que soporta la operación del software de escrutinio nacional, obteniendo análisis en tiempo real de las alertas y logs de seguridad generados por hardware y software.

3) Identificar, analizar y apoyar la remediación de los posibles impactos generados por causa de algún ataque cibernético.

4) Monitorear la infraestructura tecnológica para garantizar la seguridad de los diferentes ambientes de desarrollo, pruebas, preproducción y producción de aplicaciones.

5) Informar a la Entidad sobre recomendaciones de seguridad, tanto preventivas como correctivas, basadas en el monitoreo y la atención de eventos e incidentes.

6) Proporcionar una solución que permita la integración con plataformas tipo SOAR, a fin de obtener información adicional sobre amenazas desde múltiples fuentes y así apoyar la gestión de eventos e incidentes.

7) Soportar el servicio en una solución que permita realizar análisis heurístico sobre los eventos, con el fin de identificar comportamientos, patrones y definir reglas de correlación.

8) Soportar el servicio en una solución que cuente con técnicas avanzadas que proporcionen contexto adicional al incidente, más allá del evento reportado.

9) Generar tableros de control (Dashboards) para el SOC, que puedan ser accedidos de forma segura desde fuera de las instalaciones de la Entidad.

10) Generar como mínimo los siguientes tableros de control (Dashboards) relacionados con ciberseguridad:
   - ✓ Vista de inteligencia de amenazas.
   - ✓ Fuentes de ataque por distribución geográfica y por tipo de amenaza.
   - ✓ Eventos e incidentes detectados.
   - ✓ Eventos por segundo.
   - ✓ Métricas de acceso remoto a los servicios de la Entidad.

5.4 Copias de Respaldo y Recuperación de la Información de la Infraestructura Tecnológica

Como parte del mantenimiento correctivo y preventivo del software de escrutinio utilizado por el CNE, en la operación se recomienda realizar las siguientes actividades en relación con las copias de respaldo y la recuperación de información, para garantizar la continuidad operativa del sistema:

1) El servicio de respaldo y recuperación debe:

- **Suministrar** la infraestructura tecnológica y las licencias de software necesarias para la adecuada prestación del servicio de respaldo y recuperación de la información.
- **Permitir** la restauración o recuperación de datos en tiempos óptimos mediante una solución de backups que no supere **ocho (8) horas hábiles por terabyte (TB)**.
- **Realizar el mantenimiento** a la solución de software que permita ejecutar los procesos de restauración de aquellas copias de seguridad históricas que se generen del software de escrutinio nacional.
- **Asegurar** la planeación y el diseño de las políticas de respaldo y recuperación de información, las cuales deberán estar alineadas con la criticidad del sistema de escrutinio nacional.

2) Actividades específicas de respaldo:

a. **Administrar medios físicos o virtuales**, asegurando su integridad, confidencialidad y el acceso exclusivo al personal designado por la Entidad.
b. **Definir herramientas y procedimientos** para la toma de backups, incluyendo la especificación de la información a respaldar, periodicidad, medios de respaldo, métodos de restauración y ubicación de almacenamiento.
c. **Controlar y hacer seguimiento** a la ejecución de los respaldos, verificando el cumplimiento de los procedimientos establecidos.
d. **Ejecutar la toma de copias de respaldo** en medios físicos o virtuales que serán almacenados en un lugar distinto al de las bases de datos, conforme a las políticas de la Entidad.
e. **Revisar y registrar** las copias realizadas, manteniendo documentación clara y actualizada sobre el número y estado de las copias de seguridad en cada período.
f. **En caso de medios físicos, Recibir y enviar los medios de almacenamiento**, incluyendo las tareas de revisión, contabilización y registro en la bitácora correspondiente del transporte de los respaldos.
g. Ejecutar y verificar pruebas de respaldo y recuperación, con el fin de comprobar la funcionalidad efectiva de los backups.
h. Realizar pruebas de verificación de backups.
i. Ejecutar tareas de copiado de datos en los medios de almacenamiento y con la frecuencia que requiera la Entidad, de acuerdo con las políticas definidas.

6 Requerimientos de Soporte Técnico y Centro de Servicios TI

6.1 Soporte Técnico

El operador del servicio debe gestionar, administrar, mantener y brindar soporte técnico a la infraestructura tecnológica que provee los servicios TIC necesarios para la solución informática destinada a la consolidación de la información pertinente al Escrutinio a cargo del Consejo Nacional Electoral.

1) Niveles de Atención

Con el fin de garantizar una adecuada gestión del soporte técnico y mantenimiento del software de escrutinio a cargo del CNE, se establecen los niveles de atención que definirán los tiempos de respuesta, prioridad y resolución de los incidentes y requerimientos. Estos niveles permitirán organizar y priorizar las actividades del equipo de operación y soporte técnico, asegurando así la continuidad operativa y la calidad en la prestación del servicio conforme a los estándares y necesidades del Consejo Nacional Electoral.

NIVEL DE ATENCIÓN	NECESIDADES DE SERVICIO	ALCANCE
3	Soporte al Software para la Comisión escrutadora Nacional	Atención a incidencias y requerimientos que el software de escrutinio nacional requiera según peticiones recibidas por parte de la supervisión.
2	Gestión de Infraestructura Tecnológica en sitio	Conocimientos técnicos en un nivel avanzado, está compuesto por especialistas de infraestructura de TIC. Apoya el nivel 1, cuando éstos no logran solucionar los casos y soporta la continuidad de los servicios de TIC de la Entidad en todas las actividades descritas en el presente Anexo técnico
1,2	Monitoreo desde las Instalaciones del proveedor	Centro de Operaciones de mesa de ayuda y Centro de Operaciones de Seguridad (SOC) con el fin de anticipar y actuar de manera proactiva ante cualquier situación de seguridad que afecte la disponibilidad del servicio del software de escrutinio para la comisión escrutadora nacional

2) Medios de Contacto

El operador del servicio se obliga a cumplir con las siguientes disposiciones relacionadas con los medios de contacto para la atención de requerimientos:

a) **Disponer y operar una mesa de ayuda de primer nivel** destinada a atender todos los requerimientos que sean acordados previamente con la Entidad, durante la realización del escrutinio nacional de las elecciones de Congreso y Presidente 2026.

b) **Gestionar las solicitudes recibidas en los niveles 2 y 3** una vez que hayan sido registradas y escaladas desde el nivel 1, asegurando su adecuada resolución.

c) En caso de recibir solicitudes de manera directa en cualquier nivel, **registrar, documentar y gestionar todas dichas solicitudes** conforme a los procedimientos establecidos.

d) Garantizar que todas las solicitudes sean **registradas por el responsable designado por la Entidad**, quien tendrá a su cargo la recopilación y seguimiento de las necesidades reportadas.

e) Facilitar la recepción de solicitudes de mesa de ayuda de TI relacionadas con el sistema de escrutinio nacional, a través de los siguientes medios de contacto:

- Línea telefónica con cobertura local para la ciudad de Bogotá.
- Correo electrónico con dominio oficial de la Entidad.
- Chat y demás mecanismos electrónicos que permitan la recepción efectiva de solicitudes, previamente acordados con la Entidad.

3) Herramienta de Gestión de Servicio

En el marco del mantenimiento y actualización del software de escrutinio utilizado por el Consejo Nacional Electoral, **el prestador del servicio debería implementar, operar y mantener una herramienta de gestión de servicios de tecnologías de la información (ITSM)**, mediante la cual se realicen las labores de registro, categorización, asignación, atención, solución y cierre de todas las solicitudes asociadas con los servicios TIC de operación del sistema de escrutinio para la Comisión de Escrutinio Nacional. Durante la operación del sistema se deberá:

- Garantizar el uso adecuado de la herramienta de gestión de servicios por parte del personal autorizado.
- Asegurar la calidad, consistencia y precisión de la información procesada y registrada en dicha herramienta.
- Actualizar y mantener el inventario de componentes del sistema durante la operación en producción del sistema.

- Adicionalmente, se debe garantizar que la herramienta ITSM: Cuente con un **componente de mesa de servicios (Service Desk)**, que incluya módulos para la gestión de:

✓ Catálogo de servicios
✓ Incidentes
✓ Requerimientos
✓ Problemas
✓ Gestión de Cambios
✓ Niveles de servicio

- Permita el acceso simultáneo de al menos tres (3) agentes nominales.

- Brinde cobertura a una base de usuarios de mínimo cien (100) personas.

- Igualmente, la herramienta deberá contar con un **componente de inventario**, que incluya módulos para la gestión de configuración y activos de servicio, y que actúe como repositorio de información relacionada con:

✓ Hardware
✓ Software
✓ Documentación
✓ Servicios
✓ Usuarios, entre otros

6.2 Recurso humano especializado

Para la implementación y operación de la solución, se recomienda contar como mínimo, con el recurso humano especializado que se detalla a continuación:

PERFIL	CANTIDAD	REQUISITOS
Gerente de Proyecto	1	Profesional en ingeniería de sistemas o eléctrica o electrónica o industrial o telecomunicaciones o teleinformática o informática con especialización o maestría en Gerencia de Proyectos o Administración de proyectos o Gestión de Proyectos o Evaluación de Proyectos o en Redes de Computadores o Telecomunicaciones o en áreas relacionadas a las tecnologías de la información. Contar con certificación vigente de PMP o su equivalente. Con experiencia profesional general de mínimo 5 años y

PERFIL	CANTIDAD	REQUISITOS
		específica en gerencia de proyectos electorales de al menos 2 eventos.
Especialista en operaciones de Tecnología	1	Profesional en ingeniería de sistemas o teleinformática o informática o eléctrica o electrónica o telecomunicaciones o Administración de Sistemas de Información, responsable del apoyo logístico y soporte técnico a la implementación del Software, con certificación ITIL o COBIT nivel intermedio o con posgrado en Gerencia de Proyectos. Con experiencia general de 5 años en su carrera profesional y específica de al menos 2 años dirigiendo equipos de soporte técnico o mesa de ayuda TI.
Especialista en seguridad de la información	1	Profesional en ingeniería de sistemas o teleinformática o informática o industrial o telecomunicaciones o Administración de Sistemas de Información o Administración de Empresas, responsable de la gestión de eventos e incidentes, vulnerabilidad y monitoreo de la seguridad. Certificado como auditor ISO 27001 o CISM o CISSP o certificación equivalente o posgrado en Seguridad de la Información. Con experiencia en cargos de Consultor u Oficial de Seguridad de la información de al menos 2 años.
Soporte técnico en sitio	3	Técnico o tecnólogo en Ingeniería (Sistemas o afines). Con experiencia específica en al menos 1 proceso electoral o escrutinio

REGISTRADURÍA
NACIONAL DEL ESTADO CIVIL

INDRA COLOMBIA S.A.S.