INDICE

INDICE 1
ANEXO TÉCNICO 4
REQUERIMIENTOS GENERALES 4
1. RESPALDO Y RESTAURACIÓN CON CAPACIDAD DE 150 TB 4
1.1. Descripción General del Servicio 4
1.2. Infraestructura y Componentes a Respaldar 4
1.3. Requerimientos Técnicos del Servicio 5
1.3.1. Tipos de Respaldo 5
1.3.2. Frecuencia de Respaldo y Políticas de Retención 5
1.3.3. Requisitos de Disponibilidad y Recuperación 5
1.3.4. Requisitos de Software y Seguridad 5
1.3.5. Identificación y Documentación de los Respaldos 6
1.4. Entrega y Administración de la Información 7
1.5. Requisitos del Almacenamiento de Respaldo 7
1.6. Requisitos de Personal y Supervisión 7
1.7. Consideraciones Finales 8
2. SERVICIO DE SEGURIDAD PARA LA PROTECCIÓN DE LOS APLICATIVOS DEL CNE 8
2.2. Alcance del Servicio 8
2.2.1. Controles de Seguridad en la Infraestructura 8
2.2.2. Monitoreo y Respuesta ante Incidentes 9
2.2.3. Evaluación de Seguridad y Protección Perimetral 9
2.2.4. Seguridad de Redes y Protección contra Amenazas Externas 10
2.3. Servicio de Firewall para Aplicaciones Web 10
2.3.1. Características y Funcionalidades 10
2.3.2. Mecanismos de Protección y Detección de Amenazas 12
2.4. Servicio DDoS (Denegación de Servicio Distribuido) 12
2.5. Ethical Hacking y Pruebas de Seguridad 14

2.6. Entregables y Reportes 14
2.6.1. Reportes de Seguridad 14
2.6.2. Requisitos de Cumplimiento y Normatividad 14
2.7. Consideraciones Finales 15
3. SERVICIO DE MONITOREO DE SEGURIDAD Y ANÁLISIS DE VULNERABILIDADES
15
3.2. Requisitos Técnicos del Servicio 15
3.2.1. Monitoreo de Desempeño, Seguridad y Disponibilidad 15
3.2.2. Acceso y Configuración del Sistema de Monitoreo 16
3.2.3. Despliegue del Agente de Monitoreo 16
3.2.4. Operación del Sistema de Monitoreo 17
3.3. Servicio de Análisis de Vulnerabilidades 20
3.3.1. Alcance del Escaneo de Vulnerabilidades 20
3.3.2. Frecuencia y Ejecución del Escaneo 20
3.3.3. Reportes y Entregables 20
3.4. Requisitos de Seguridad y Cumplimiento 21
3.5. Consideraciones Finales 21
4. SERVICIO DE REPLICACIÓN, COLOCATION Y COMUNICACIONES DE INFRAESTRUCTURA TECNOLÓGICA DEL CNE 22
4.1. Replicación de Infraestructura Crítica 22
4.1.1. Descripción del Servicio 24
4.1.2. Requisitos Técnicos 24
4.1.3. Especificaciones Técnicas de Cómputo 24
4.1.4. Línea Base de Infraestructura a Replicar 25
4.2. Servicio de Colocation 25
4.2.1. Equipos que colocar en el DataCenter 25
4.2.2. Sistemas Operativos y Motores de Bases de Datos 25
4.3. Comunicaciones y Redes 26
4.3.1. Características de Red 26
4.3.2. Recursos en DataCenter (ACTUAL CNE) 26

4.3.3. Interconexión entre Sedes 26
4.3.4. Gestión de Tráfico y Balanceo 27
4.4. Ciberseguridad 27
4.5. Consideraciones Finales 28
5. MESA DE AYUDA 28
5.1. Obligaciones específicas 28
5.2. Reportes 29
5.3. Tiempo de Atención a Fallas 29
6. GARANTÍA DE CONTINUIDAD DEL SERVICIO 37
6.1. Transición sin Costo para el CNE 38
6.2. Plan de Transición Detallado 38
6.3. Servicios Cubiertos por la Transición 38
6.4. Mesa de Ayuda 39
6.5. Condiciones sobre la Infraestructura Existente 39
6.6. Garantía de Continuidad Operativa 39
6.7. Compromiso de No Afectación 39
6.8. Supervisión y Seguimiento 40
6.9. Acuerdo Complementario 40
7. ANS 40

ANEXO TÉCNICO

El Consejo Nacional Electoral se encuentra adelantando proceso de estudio de mercado, donde se detalla los requerimientos técnicos necesarios para una solución tecnológica integral enfocada en el aseguramiento y disponibilidad de los distintos elementos de hardware y software que soportan los aplicativos misionales del CNE

REQUERIMIENTOS GENERALES

1. RESPALDO Y RESTAURACIÓN CON CAPACIDAD DE 150 TB

1.1. Descripción General del Servicio

El servicio de respaldo y restauración debe garantizar la seguridad, integridad y disponibilidad de la información almacenada en los sistemas críticos del Consejo Nacional Electoral (CNE). La solución debe ser altamente confiable, automatizada y eficiente, permitiendo la ejecución de tareas de respaldo y restauración conforme a una política establecida.

El sistema de respaldo debe soportar un almacenamiento total de 150 TB, permitiendo la protección de los sistemas misionales del CNE, asegurando la continuidad operativa ante fallos, desastres o ataques cibernéticos.

1.2. Infraestructura y Componentes a Respaldar

El servicio debe incluir la protección y respaldo de la siguiente infraestructura tecnológica:

- Servidores de aplicaciones y bases de datos misionales del CNE.
- Servidores de almacenamiento compartido.
- Equipos de red y seguridad perimetral.
- Sistemas de gestión documental y plataformas ERP.
- Repositorios de información y carpetas compartidas.
- Servidores de autenticación y balanceo de carga.
- Servidores proxy reverso y controladores de dominio.
- Sistemas de respaldo de cuentas de correo para 700 usuarios.
- Bases de datos en producción con motores SQL Server y PostgreSQL.
- Aplicaciones críticas para la gestión de procesos electorales y administrativos.

1.3. Requerimientos Técnicos del Servicio

1.3.1. Tipos de Respaldo

El sistema debe permitir la ejecución de diferentes tipos de respaldos, incluyendo:

- Respaldo Completo: Copia de toda la información almacenada en los servidores.
- Respaldo Incremental: Copia de los cambios acumulados desde el último respaldo completo.
- Respaldo Diferencial: Captura de los cambios acumulados desde el último respaldo completo.
- Respaldo a Medio Externo (Opcional): Transferencia de copias a almacenamiento fuera del entorno de producción.

1.3.2. Frecuencia de Respaldo y Políticas de Retención

- El servicio debe cumplir con los siguientes parámetros de ejecución y retención:
- Respaldos incrementales diarios
- Almacenamiento de respaldos offsite en una ubicación externa segura para la protección ante desastres.

1.3.3. Requisitos de Disponibilidad y Recuperación

La solución debe cumplir con los siguientes acuerdos de nivel de servicio (SLA):

- RTO (Recovery Time Objective): Máximo de 24 horas para recuperación de datos.
- RPO (Recovery Point Objective): Máximo de 4 horas para garantizar la integridad de la información.

1.3.4. Requisitos de Software y Seguridad

El proveedor debe suministrar el software necesario para la ejecución de los respaldos.

- Soporte para técnicas avanzadas de deduplicación y compresión de datos.
- Cifrado de la información almacenada con algoritmos de seguridad estándar (AES-256).
- Implementación de mecanismos de control de acceso y autenticación multifactor (MFA).
- La solución debe leer y verificar automáticamente la consistencia de los datos en el archivo de copia de seguridad una vez completada la copia de seguridad. En caso de que se detecte corrupción de datos, la solución debe reconstruir automáticamente el bloque dañado con los datos reales.
- La solución debe proporcionar una copia de seguridad eficiente "incremental para siempre" e incluir opciones de copias de seguridad completas y ad-hoc para

cualquiera que sea la carga objetivo (VM Onpremises, VM Cloud Publica, NAS, Servidor Fisico).

- La solución debe detectar automáticamente los snapshots huérfanos generados por VMWare o la misma solución de respaldos y ejecutar de manera automática un proceso que permita su consolidación de forma consistente.
- La solución deberá permitir la creación de backup full sintéticos para máquinas virtuales del ambiente virtual de VMWare vSphere sin importar el sistema operativo de la máquina objetivo (Linux - Windows).
- La solución no debe requerir agentes implementados en máquinas virtuales para facilitar el respaldo de aplicaciones y la ejecución de tareas de recuperación granular de aplicaciones.
- Los respaldos sin agente de máquinas virtuales deben proporcionar respaldo de logs o archivos de transacciones de Microsoft SQLServer y Oracle Database junto con copias de seguridad basadas en snapshots.
- La solución debe utilizar la tecnología Changed Block Tracking para copias de seguridad incrementales de cargas de trabajo físicas o basadas en la nube.
- La solución debe proporcionar tecnología de recuperación de respaldo de máquinas virtuales y máquinas fisicas x86 de forma instantánea (encendido en menos de 5 minutos y automática) sobre la infraestructura VMWare vSphere desde el repositorio de respaldos ya sea que se encuentren Onpremises o sobre un almacenamiento de Objetos en una nube.
- La solución debe poder utilizar la copia de seguridad o réplica de la máquina virtual para iniciar la máquina virtual en un entorno de red aislado para fines de prueba o certificación de respaldos.
- La solución debe proporcionar la tecnología de recuperación Changed Block Tracking para máquinas virtuales VMware, es decir, tener la capacidad de recuperar solo los bloques modificados desde el último respaldo y no la VM completa.
- La solución debe poder escanear los datos de la máquina virtual a recuperar con un software antivirus antes de iniciar la restauración de la máquina al entorno de producción de forma integrada y automática. La solución debe abortar la operación de recuperación si se detecta malware.
- La solución debe ofrecer inmutabilidad para el repositorio Onpremises de primer nivel y de almacenamiento de objetos de forma nativa.
- Monitoreo en tiempo real de los procesos de respaldo con generación de alertas.
- Gestión centralizada del servicio mediante una consola unificada.
- Implementación de auditoría y trazabilidad de accesos y operaciones.

1.3.5. Identificación y Documentación de los Respaldos

Cada respaldo deberá estar debidamente identificado y documentado con los siguientes datos:

- Fecha y hora de ejecución.
- Servidor y sistema origen del respaldo.
- Estado del respaldo (exitoso, parcialmente exitoso, fallido).
- Reporte detallado de eventos y anomalías.

1.4. Entrega y Administración de la Información

- El proveedor debe garantizar la disponibilidad de los respaldos durante un (1) mes posteriores a la finalización del contrato para facilitar la migración o recuperación de datos por parte del CNE.
- Se debe entregar la información en el formato original de los archivos respaldados.
- Se debe disponer de los medios físicos o digitales necesarios para la entrega de la información al CNE.
- Se debe proporcionar acceso con rol de administrador global al recurso de almacenamiento a un funcionario designado por el CNE.

1.5. Requisitos del Almacenamiento de Respaldo

El sistema de almacenamiento del respaldo debe cumplir con las siguientes características:

- Capacidad mínima: 150 TB.
- Tecnología de almacenamiento: Discos de estado sólido (SSD) para acceso rápido a la información.
- Debe permitir realizar deduplicación para la eliminación de datos redundantes.
- Debe permitir la funcionalidad de proporcionar compresión de datos en línea y posterior al proceso en función de reducir la cantidad de almacenamiento.
- Debe incluir predicción de tendencia de capacidad. ☐ Conectividad segura: Se debe otorgar acceso mediante VPN ☐ Interfaz de acceso: Acceso vía interfaz web, SSH o SFTP.
- Interoperabilidad: Soporte para integración con sistemas de gestión documental y bases de datos misionales del CNE.

1.6. Requisitos de Personal y Supervisión

Dado el nivel crítico de la información a respaldar, el proveedor deberá garantizar las siguientes funciones:

- Monitoreo en tiempo real de los procesos de respaldo.
- Generación de informes de estado y cumplimiento.
- Atención de incidentes y activación de procedimientos de restauración en caso de fallos.
- Implementación de alertas tempranas ante posibles fallos en el sistema de respaldo.

1.7. Consideraciones Finales

- El proveedor será responsable de la confiabilidad, disponibilidad e integridad de la información almacenada.
- Se deberá garantizar el cumplimiento de la normativa vigente en materia de protección de datos y ciberseguridad.
- El sistema deberá contar con mecanismos de recuperación ante desastres y redundancia en sitios alternativos.
- La solución debe estar alineada con los estándares de seguridad y mejores prácticas internacionales en gestión de respaldos.

2. SERVICIO DE SEGURIDAD PARA LA PROTECCIÓN DE LOS APLICATIVOS DEL CNE

2.1. Descripción General

El servicio de seguridad informática tiene como objetivo garantizar la protección integral de la infraestructura tecnológica y los aplicativos misionales del Consejo Nacional Electoral (CNE), asegurando la continuidad operativa y la mitigación de riesgos cibernéticos. La solución debe incluir mecanismos de monitoreo, detección, prevención y respuesta ante amenazas de seguridad, con un enfoque basado en estándares internacionales y mejores prácticas de Ciberseguridad.

El contratista deberá proveer los servicios y herramientas necesarias para fortalecer la seguridad de la infraestructura del CNE, con software licenciado, fabricante reconocido y contrato de soporte vigente. La ejecución del servicio deberá operar bajo un esquema 7x24, garantizando la disponibilidad de recursos especializados para la atención y gestión de incidentes de seguridad.

2.2. Alcance del Servicio

El servicio de seguridad informática deberá garantizar, como mínimo, la implementación de los siguientes controles y medidas de protección:

2.2.1. Controles de Seguridad en la Infraestructura

- Protección de la infraestructura mediante firewalls aplicaciones Web (WAF) servicio en nube.
- Monitoreo y análisis de vulnerabilidades en aplicaciones y servidores.
- Prueba de Ethical Hacking (una durante la ejecución del contrato), con análisis de penetración sobre los dominios establecidos por la supervisión del contrato (máximo 5 dominios).

- Todas las herramientas utilizadas para la ejecución de estos controles deben contar con licencias vigentes que permitan su uso legal durante el periodo de contratación.
- Operador tecnológico debe mantener vigente durante la operación de su servicio la solución de Firewall Perimetral.

2.2.2. Monitoreo y Respuesta ante Incidentes

- Servicio de monitoreo continuo 7x24 con correlación de eventos de seguridad.
- Escalamiento inmediato de eventos de seguridad detectados.
- Implementación de alertas automatizadas y notificación temprana ante amenazas.
- Registro y documentación de incidentes con reportes detallados para auditoría.

2.2.3. Evaluación de Seguridad y Protección Perimetral

- Monitoreo de la seguridad perimetral, evaluando el estado de firewalls y otros dispositivos de control de acceso.
- Evaluación y pruebas de seguridad en la infraestructura on-premise del CNE, alineadas con estándares como NIST, CIS Benchmarks o ISO 27001.
- Implementación de controles de detección y prevención de intrusiones en la infraestructura del CNE.

2.2.4. Seguridad de Redes y Protección contra Amenazas Externas

- Implementación de políticas de segmentación de red y filtrado de tráfico.
- Protección contra ataques de fuerza bruta en los portales de autenticación del CNE.
- Correlación de eventos de seguridad para la detección de patrones maliciosos y posibles intrusiones.
- Integración de soluciones de filtrado de contenido y detección de phishing en la infraestructura del CNE.

2.3. Servicio de Firewall para Aplicaciones Web

El servicio de Web Application Firewall (WAF) en la nube deberá garantizar la protección de los aplicativos web del CNE. La solución debe incluir los siguientes componentes:

2.3.1. Características y Funcionalidades

- Protección de Aplicaciones Web: Prevención de ataques dirigidos a las aplicaciones del CNE, asegurando la integridad, confidencialidad y disponibilidad de la información.
- Módulo de Protección contra Fuerza Bruta: Implementación de mecanismos de bloqueo de intentos repetitivos de autenticación, con un tiempo de bloqueo configurable.
- Renovación y Soporte:
    - Renovación del soporte de firewall perimetral y de aplicaciones en la nube actualmente en operación en el CNE.
    - Soporte Nivel I y II de fábrica con cobertura 7x24, incluyendo:
        - Actualizaciones de firmware y bases de datos de amenazas.
        - Acceso al portal de soporte y asistencia técnica vía web, chat y teléfono.
- Compatibilidad con IPv6 y protocolos de seguridad modernos.
- Protección de Aplicaciones Web: Prevención de ataques dirigidos a las aplicaciones del CNE, asegurando la integridad, confidencialidad y disponibilidad de la información.
- La solución debe ser totalmente compatible con IPv6.
- Integrarse de forma nativa a la actual solución de Gestión de Logs y reportes de la entidad.
- La solución debe contar con características de Machine Learning.
- La solución de WAF debe tener la capacidad de integrarse de manera nativa con la plataforma de NGFW de la entidad
- La solución de Web Application Firewall debe tener la capacidad de enviarle las IP detectadas como maliciosas sean informadas y sea adicionada automáticamente a un grupo de direcciones IPs para que puedan ser utilizadas en las políticas de la plataforma de NGFW.

- El proveedor debe garantizar que la solución de NGFW que tiene la entidad pueda tener la capacidad de crear Widgets que le permitan visualizar los eventos del WAF
- El proveedor debe garantizar que la solución de analítica, logs y reportes que tiene la entidad debe tener la capacidad de recibir y correlacionar información del WAF
- El Numero de Aplicaciones a proteger no deberá estar limitado por licenciamiento.
- Debe incluir mínimo 5 dominios administrativos licenciados
- El licenciamiento debe incluir como mínimo los siguientes servicios de seguridad: Seguridad web, reputación IP, antimalware, Sandbox Cloud, defensa de Credential Stuffing y Threat Analytics.
- La solución debe integrar firmas de amenazas y ataques conocidos y deberá proteger de ataques nuevos o de día cero actualizándose durante el tiempo de la garantía.
- Con el fin de garantizar la integridad de las aplicaciones web, la solucion deberá contar con un módulo de anti-defacement el cual permita monitorear las aplicaciones, alertar y de ser necesario restaurar de forma automática en caso de modificaciones no autorizadas de las aplicaciones web protegidas, la solución deberá poder monitorear la integridad de los archivos por medio de FTP, SSH o SMB, por lo tanto no se acepta soluciones que requieran la instalación de agentes, los cuales agreguen más carga a los servidores.
- La solución debe contar con protección de ataques basados en la localización geográfica del atacante
- La solución debe contar con un módulo que prevenga ataques de fuerza bruta contra los portales de autenticación de la entidad, el cual permita bloquear por un periodo de tiempo al atacante, dicho periodo de tiempo deberá poder ser parametrizado por la entidad.
- La solución debe contar con dashboards, que muestren como mínimo información en tiempo real del tráfico, Historia de Ataques, sesiones por política e información del sistema.
- La solución debe soportar ambientes, donde sea posible dividir la administración y aplicar políticas de WAF para ambiente en producción y desarrollo o las que decida la entidad.
- La solución debe permitir la creación de reglas de autenticación, dichas reglas de autenticación deberán permitir:
    - o Autenticación por medio de LDAP o Radius. o Autenticación de doble factor por medio de Token. o (SSO) Single Sign-On para portales tales como OWA, SharePoint, etc. □ La administración y gestión de la plataforma debe permitir:
    - o Visibilidad de aplicaciones Cloud usadas por el usuario.
    - o Visibilidad de los sitios web más consultados por los usuarios.
- Visibilidad de las amenazas que han ocurrido en la red.
- Renovación y Soporte:
    - o Renovación del soporte de firewall perimetral y Solucion de Web Application Firewall (WAF) durante la vigencia del contrato de operación en el CNE.

- Soporte Nivel I y II de fábrica con cobertura 7x24, incluyendo:
- Acceso al portal de soporte y asistencia técnica vía web, chat y teléfono.

- El oferente deberá realizar la instalación y configuración de los equipos con personal certificado por el fabricante con el cual se esté presentando.
- El proponente deberá aportar carta del fabricante de la solución ofertada dirigida al presente proceso indicando el nivel de Partner del proponente.
- El proponente debe adjuntar una carta de compromiso donde manifieste inequívocamente el cumplimiento técnico de los mínimos requeridos indicando tecnología ofertada

2.3.2. Mecanismos de Protección y Detección de Amenazas

- Protección contra ataques de día cero mediante:
  - Firmas de amenazas y patrones de ataque conocidos.
  - Análisis de comportamiento basado en inteligencia artificial (IA) y Machine Learning (ML) para la detección de nuevas amenazas.

- Filtrado Web y Seguridad en la Navegación:
  - Implementación de políticas de control de acceso a contenidos web.
  - Análisis de tráfico web en tiempo real para prevenir accesos no autorizados.
  - Monitoreo de tráfico cifrado y descifrado selectivo para identificar ataques encubiertos en SSL/TLS.

2.4. Servicio DDoS (Denegación de Servicio Distribuido).

Servicio sistema de seguridad informática para Controlar los ataques de denegación de servicio distribuido que puedan ser realizados contra la infraestructura de seguridad perimetral de la entidad, mediante una plataforma de propósito específico y diversos sistemas de filtrado y establecimiento de umbrales, geolocalización y demás características de funcionamiento solicitadas en el presente documento.

- Todos los componentes del sistema: procesador, tarjeta principal y en general el conjunto electrónico debe ser propósito específico.
- Para el sistema de contención de ataques, NO se aceptan sistemas de propósito general (PCs o servidores) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux.

- La plataforma es requerida por la duración del contrato en un esquema 7 x 24 ante fabricante.
- La solución de contención y mitigación de ataques de denegación de servicio distribuido deberá contar con las siguientes características de rendimiento:
    - Desempeño: 8 Gbps
    - Espacio en disco de al menos 480 GB o Soportar al menos 8.8 Mpps o Fuentes simultáneas mínimo 1 millón o Soportar hasta 2 M queries DNS por segundo o La latencia típica debe ser menor a 70 us
- Proporcionar una solución de propósito específico y dedicado para la entidad la cual permita el aseguramiento del acceso desde internet hacia la infraestructura pública de la entidad, contra ataques especializados de Denegación de Servicio Distribuido.
- La solución de denegación de servicios debe tener la capacidad de enviarle las IP detectadas como maliciosas sean informadas y sea adicionada automaticamente a un grupo de direcciones IPs para que puedan ser utilizadas en las políticas de la plataforma de NGFW de la entidad.
- Deberá garantizar que se comporta como un bridge capa 2 el cual no deberá realizar ningún tipo de modificación en los paquetes, la IP o las MAC involucradas en la transmisión de los datos.
- El equipo propuesto debe tener mecanismos de mitigación de ataques en la capa 3, contra grandes volúmenes de tráfico (floods)
- El proveedor debe garantizar que la solución de analítica, logs y reportes que tiene la entidad debe tener la capacidad de recibir y correlacionar información de AntiDDoS
- La solución de denegación de servicios debe tener la capacidad de enviarle las IP detectadas como maliciosas sean informadas y sea adicionada automáticamente a un grupo de direcciones IPs para que puedan ser utilizadas en las políticas de la plataforma de NGFW.
- El producto debe admitir el registro de protocolo abierto para el procesamiento ascendente de registros de ataques y eventos.
- Los gráficos de monitoreo de paquetes descartados se deben mostrar al menos en la capa 3, capa 4 y capa 7.
- El equipo debe ser capaz de enviar correos electrónicos para las alertas del sistema
- La solución debe tener capacidad de auto aprendizaje para adaptar políticas basadas en comportamiento.
- La detección deberá ser basada en el análisis del comportamiento de los patrones de tráfico de ataques (No dependerá de actualizaciones de firmas digitales)
- El oferente deberá realizar la instalación y configuración de los equipos con personal certificado por el fabricante con el cual se esté presentando.
- El oferente deberá aportar los documentos, datasheet y/o catálogos de las soluciones ofertadas,

- El proponente debe adjuntar una carta de compromiso donde manifieste inequívocamente el cumplimiento técnico de los mínimos requeridos indicando tecnología ofertada

2.5. Ethical Hacking y Pruebas de Seguridad

El servicio deberá incluir una prueba de Ethical Hacking durante la ejecución del contrato, la cual debe cumplir con los siguientes lineamientos:

- Pruebas de penetración en aplicaciones web, infraestructura y redes.
- Análisis de configuraciones inseguras y exposición de información sensible.
- Evaluación de cumplimiento de estándares internacionales como OWASP, MITRE ATT&CK y NIST 800-53.
- Generación de reportes detallados con evidencia técnica, nivel de riesgo y recomendaciones de mitigación.

2.6. Entregables y Reportes

El contratista deberá entregar los siguientes reportes y documentación:

2.6.1. Reportes de Seguridad

1. Informe de Monitoreo de Seguridad (mensual):
   - Eventos críticos detectados.
   - Análisis de incidentes de seguridad.
   - Medidas correctivas implementadas.
2. Reporte de Evaluación de Seguridad Perimetral (trimestral):
   - Estado de la infraestructura de seguridad del CNE.
   - Análisis de configuraciones y cumplimiento de mejores prácticas.
   - Recomendaciones de mejora.
3. Informe de Pruebas de Ethical Hacking:
   - Metodología aplicada y alcance de las pruebas.
   - Vulnerabilidades detectadas y nivel de criticidad.
   - Plan de remediación y mitigación.

2.6.2. Requisitos de Cumplimiento y Normatividad

- ISO 27001: Implementación de controles de seguridad de la información.
- NIST 800-53: Cumplimiento con estándares de ciberseguridad para infraestructuras críticas.
- OWASP Top 10: Mitigación de riesgos en aplicaciones web.
- GDPR/LGPD: Protección de datos personales en entornos digitales.

2.7. Consideraciones Finales

- El contratista será responsable de la integridad y disponibilidad del servicio de seguridad.
- El servicio de monitoreo y respuesta debe garantizar una disponibilidad del 99.95%.
- Todas las actividades deben ejecutarse conforme a las políticas de seguridad definidas por el CNE.
- La solución debe integrarse con la infraestructura existente sin requerir cambios disruptivos.

---

3. SERVICIO DE MONITOREO DE SEGURIDAD Y ANÁLISIS DE VULNERABILIDADES

3.1. Descripción General

El servicio de monitoreo de seguridad y análisis de vulnerabilidades tiene como objetivo garantizar la disponibilidad, integridad y desempeño de los servidores que soportan los aplicativos misionales y de apoyo del Consejo Nacional Electoral (CNE). Esta solución debe permitir la supervisión en tiempo real del estado de la infraestructura tecnológica, asegurando la detección temprana de amenazas y vulnerabilidades para minimizar riesgos operativos y de ciberseguridad.

El contratista deberá proveer acceso a la plataforma de monitoreo al personal designado por el CNE, asegurando visibilidad y control sobre los sistemas monitoreados. La solución deberá operar bajo un esquema 7x24 y estar alineada con las mejores prácticas de seguridad, cumplimiento normativo y gestión de riesgos.

3.2. Requisitos Técnicos del Servicio

3.2.1. Monitoreo de Desempeño, Seguridad y Disponibilidad

El sistema de monitoreo deberá cumplir con los siguientes requisitos:

- Supervisión en tiempo real del estado y disponibilidad de los servidores.
- Servicios de monitoreo y correlación de eventos de seguridad sobre la plataforma SIEM, para 100 dispositivos (FIM) y 4000 EPS (eventos por segundo). □ SERVIDORES:
  - Servidores Windows: 15 Servidores físicos e instancias de máquina virtual
  - Servidores Linux: 10 Servidores físicos e instancias de máquina virtual

- Hipervisores: 5 Nodos de Administración ESX □ DISPOSITIVOS DE RED:
- Firewalls: 3 Firewalls FortiGate o Switch Core: 2 Switch Core Switches de Acceso: 50 Switches de Acceso o Plataformas WIFI: 48 Access Points

- Medición de consumo de recursos de hardware, incluyendo:
- Procesador (CPU): porcentaje de utilización y carga promedio.
- Memoria RAM: uso total, picos de consumo y procesos principales.
- Almacenamiento: utilización del disco, tiempos de respuesta y fragmentación.
- Conectividad y Red: latencia, pérdida de paquetes, tráfico de entrada/salida y disponibilidad de interfaces.
- Implementación de alertas automáticas ante fallos o anomalías en el desempeño de los servidores.
- Registro histórico de métricas para análisis de tendencias y optimización de infraestructura.
- El proponente deberá aportar carta del fabricante de la solución ofertada dirigida al presente proceso indicando el nivel de Partner del proponente.
- El proponente debe adjuntar una carta de compromiso donde manifieste inequívocamente el cumplimiento técnico de los mínimos requeridos indicando tecnología ofertada

3.2.2. Acceso y Configuración del Sistema de Monitoreo

Para garantizar la consulta y análisis de los servidores monitoreados, el contratista deberá:

- Configurar un servidor proxy SNMP en el centro de datos del CNE con una Management Information Base (MIB) adecuada al volumen de información procesada.
- Garantizar que el CNE tenga acceso permanente y sin restricciones a la plataforma de monitoreo.
- Implementar mecanismos de autenticación segura para el acceso a la plataforma, asegurando confidencialidad e integridad de los datos.
- Establecer roles y permisos de usuario para la gestión de consultas y reportes dentro del sistema.

3.2.3. Despliegue del Agente de Monitoreo

El contratista será responsable de la implementación de agentes de monitoreo en cada uno de los servidores bajo el alcance del contrato. Este proceso se compone de dos fases:

- Instalación del Agente de Monitoreo

    - Implementación del software en cada servidor conforme a los manuales del fabricante.
    - Configuración de los agentes para la recolección y transmisión de datos a la plataforma central.
    - Verificación de compatibilidad con sistemas operativos y aplicaciones instaladas.
- Validación del Monitoreo o Registro de los servidores dentro del sistema de monitoreo con acceso a internet.
    - Pruebas de conectividad y reporte de eventos en tiempo real. o Confirmación de correcta recepción de datos y generación de alertas.

3.2.4. Operación del Sistema de Monitoreo

El servicio de monitoreo deberá incluir la administración y operación continua de la plataforma existente en el CNE bajo un esquema 7x24, asegurando:

- Detección temprana de incidentes de seguridad y fallos de infraestructura.
- Registro y correlación de eventos en un Security Information and Event Management (SIEM).
- Integración con la infraestructura de seguridad perimetral del CNE para una gestión unificada.
- Generación de reportes automáticos sobre el estado de seguridad y disponibilidad de los sistemas.
- Mantener el inventario actualizado de dispositivos monitoreados de la solución en la cual se basa el servicio de Monitoreo, deberá incluir el descubrimiento de dispositivos (Activos TI) de infraestructura automatizado, al igual, que el registro de estos dispositivos (Activos TI) en una base de datos de administración de configuraciones (CMDB).
- La solución de correlación de eventos (SIEM) debe garantizar analítica de red en tiempo real seguridad y conformidad listas para usar un único panel de administración, arquitectura a escala de la nube, autoaprendizaje del inventario de activos (cmdb),la solución debe ser licenciada y dedicada para la entidad. no se admiten entornos compartidos ni multitenant.
- Asignaciones de reglas de TI e ICS de MITRE ATT&CK y visibilidad de la cobertura.
- El SIEM debe tener la capacidad de proporcionar a los Next Generation Firewalls que tiene la entidad, las direcciones IP que se han asociado con actividades sospechosas o maliciosas.

- El SIEM debe garantizar disponibilidad de un conjunto de respuestas pre-configuradas ante eventos de seguridad, de manera que se permita no sólo la detección sino también la remediación automatizada ante determinadas amenazas.
- Actualización continua del contexto, de los dispositivos, su software y parches instalados, así como los servicios en ejecución.
- Análisis del rendimiento de aplicaciones y sistemas junto con datos del entorno para identificar rápidamente problemas de seguridad.
- Contexto de usuario, en tiempo real, con seguimiento de direcciones IP, cambios de identidad de usuario, contexto de datos de ubicación física y geolocalización.
- Detectar dispositivos, aplicaciones de red y cambios de configuración no autorizados.
- El SIEM debe ofrecer múltiples formas de monitorear los Next Generation Firewalls que tiene la entidad, soportando como mínimo el descubrimiento a través de API REST, Syslog, Netflow, SNMP y SSH.
- El SIEM debe garantizar Informes predefinidos listos para ser utilizados, que soporten una amplia gama de necesidades de auditoría y cumplimiento normativo.
- El SIEM debe garantizar como mínimo la supervisión de configuraciones en tiempo real para:
    - Recopilar archivos de configuración de red, almacenados en un repositorio versionado.
    - Recopilar las versiones de software instaladas, almacenadas en un repositorio versionado.
    - Detección automatizada de cambios en la configuración de la red y el software instalado.
    - Detección automatizada de cambios de archivos y carpetas - Windows y Linux - quién y qué.
    - Detección automatizada de cambios desde un archivo de configuración.
    - Posibilidad de detección automatizada de cambios en el registro de Windows a través de agente.
- El SIEM debe garantizar la integración con fuente de alimentación externa con:
    - Búsqueda de eventos en real - sin necesidad de indexación.
    - Búsquedas por palabras clave basadas en atributos de eventos analizados.
    - Búsqueda de eventos históricos - consultas de tipo SQL con condiciones de filtro booleanas, agrupar por agregaciones relevantes, filtros de hora del día, concordancia de expresiones regulares, expresiones calculadas - GUI y API.
    - Match de patrones complejos en tiempo real.
    - Uso de objetos CMDB y datos de usuario/identidad y ubicación en búsquedas y reglas.
    - Programación de informes y entregas de resultados por correo electrónico a los principales interesados.
    - Posibilidad de personalización de los informes, tanto en contenido como en aspecto (portadas, textos, imágenes, etc.).

- Búsqueda de eventos en toda la organización o en el ámbito de un dominio físico o lógico.
- Listas de vigilancia dinámicas para hacer un seguimiento de los infractores críticos - con la posibilidad de usar listas de vigilancia en cualquier regla de generación de informes.
- Análisis escalable mediante la adición de nodos worker en caliente.
- Posibilidad de priorización de los informes de incidentes.

- El SIEM debe garantizar analítica en:
  - Búsqueda de eventos en real - sin necesidad de indexación.
  - Búsquedas por palabras clave basadas en atributos de eventos analizados.
  - Búsqueda de eventos históricos - consultas de tipo SQL con condiciones de filtro booleanas, agrupar por agregaciones relevantes, filtros de hora del día, concordancia de expresiones regulares, expresiones calculadas - GUI y API.
  - Match de patrones complejos en tiempo real.
  - Uso de objetos CMDB y datos de usuario/identidad y ubicación en búsquedas y reglas.
  - Programación de informes y entregas de resultados por correo electrónico a los principales interesados.
  - Posibilidad de personalización de los informes, tanto en contenido como en aspecto (portadas, textos, imágenes, etc.).
  - Búsqueda de eventos en toda la organización o en el ámbito de un dominio físico o lógico.
  - Listas de vigilancia dinámicas para hacer un seguimiento de los infractores críticos - con la posibilidad de usar listas de vigilancia en cualquier regla de generación de informes.
  - Análisis escalable mediante la adición de nodos worker en caliente. o Posibilidad de priorización de los informes de incidentes.
- El licenciamiento ofertado deberá disponer de un método de licenciamiento escalable tanto por número de dispositivos como por EPS asociados, pudiendo elegir al menos entre licencias perpetuas y modo suscripción.
- Se deberá disponer de paquetes de licencia de agentes avanzados para monitorización de servidores críticos Windows y Linux, tanto en modo perpetuo como modo suscripción.
- Se deberá disponer de otras suscripciones como Indicadores de Compromiso (IoC).
- Se deberá poder añadir EPS adicionales sin necesidad de contratar soporte asociado a los mismos.
- Se podrán desplegar tantos colectores virtuales como se quiera sin coste adicional.

3.3. Servicio de Análisis de Vulnerabilidades

3.3.1. Alcance del Escaneo de Vulnerabilidades

El servicio de análisis de vulnerabilidades deberá realizar evaluaciones de seguridad a los activos tecnológicos del CNE, incluyendo servidores, aplicaciones y dispositivos de red. Este proceso debe cumplir con los siguientes requisitos:

- El contratista debe realizar un escaneo de vulnerabilidades que permita obtener los resultados en tiempo real y a través de una consola web, donde se pueda gestionar y monitorear los avances de las vulnerabilidades a 50 activos de información que la entidad defina, este podrá realizarse con una herramienta de fabricante licenciada u open source a escogencia del proveedor. El mínimo de escaneos será uno (1) por mes, los cuales se realizarán en coordinación con la supervisión del contrato de tal manera que se garantice que esta operación no causara afectaciones a la correcta operación de los servicios del CNE.
- Identificación de vulnerabilidades conocidas (CVE) y configuraciones inseguras.
- Evaluación de cumplimiento con estándares de seguridad (NIST, CIS Benchmarks, ISO 27001).
- Reporte detallado de vulnerabilidades categorizadas según su criticidad (Alta, Media, Baja).

3.3.2. Frecuencia y Ejecución del Escaneo

El contratista deberá realizar un mínimo de un (1) escaneo mensual, coordinado con la supervisión del contrato para evitar afectaciones en los servicios del CNE. El proceso debe considerar:

- Escaneos en ambientes de producción con impacto mínimo en la operación.
- Posibilidad de programar escaneos en horarios no críticos.
- Todas las herramientas empleadas para el desarrollo de estas actividades deben contar con una licencia vigente que autorice su uso.

3.3.3. Reportes y Entregables

Como resultado de los análisis de vulnerabilidades, el contratista deberá entregar los siguientes informes:

- Informe Ejecutivo
- Resumen de hallazgos críticos y tendencias.
- Evaluación de impacto sobre la operación del CNE.
- Recomendaciones estratégicas para mitigación de riesgos.
- Reporte Técnico Detallado
- Listado completo de vulnerabilidades detectadas.

- Clasificación por nivel de riesgo (Crítico, Alto, Medio, Bajo).
- Análisis de posibles vectores de explotación.
- Priorización de vulnerabilidades a corregir.
- Estrategia de mitigación y cierre de brechas de seguridad.

3.4. Requisitos de Seguridad y Cumplimiento

El servicio debe estar alineado con estándares de seguridad reconocidos y mejores prácticas internacionales, incluyendo al menos las siguientes:

- ISO 27001: Gestión de seguridad de la información.
- NIST 800-53: Controles de ciberseguridad para infraestructuras críticas.
- OWASP Top 10: Mitigación de riesgos en aplicaciones web.
- GDPR/LGPD: Protección de datos personales en entornos digitales.

Se deberán implementar medidas de seguridad perimetral, cifrado de datos en tránsito y almacenamiento seguro de logs de monitoreo y análisis de vulnerabilidades.

3.5. Consideraciones Finales

- El contratista será responsable de la confiabilidad, integridad y disponibilidad de la información generada por el sistema de monitoreo.
- Se deberá garantizar un porcentaje de disponibilidad del servicio de monitoreo entre el 99.9% y 99.95%.
- El CNE tendrá acceso total a la plataforma de monitoreo y control sobre la ejecución de escaneos de vulnerabilidades.
- Todas las actividades deben ejecutarse conforme a las directrices del Centro de Seguridad Digital del CNE y la supervisión del contrato.

4. SERVICIO DE REPLICACIÓN, COLOCATION Y COMUNICACIONES DE INFRAESTRUCTURA TECNOLÓGICA DEL CNE

4.1. Replicación de Infraestructura Crítica

Se requiere replicar un total de 40 máquinas virtuales, que están contenidas en los servidores de hyperconvergencia

Nombre	rol	Estado	Condición	Espacio aprovisionado	Espacio utilizado	moria de host
DeployHP	Servidor de despliegue de máquinas hiperconvergencia	Encendido	Normal	100 GB	84,55 GB	12,9 GB
GSMP16_Gateway	Puerta de enlace análisis de vulnerabilidades	Encendido	Normal	52,48 GB	5,54 GB	4,78 GB
GSMP_Gateway_192	Puerta de enlace análisis de vulnerabilidades	Encendido	Normal	50 GB	4,05 GB	3,4 GB
HPE-ARBITER	broker hyperconvergencia	Encendido	Normal	90 GB	46,69 GB	8,06 GB
OmniStackVC-10-0-2-14	controlador hyperconvergencia	Encendido	Normal	210,05 GB	13,24 GB	72,27 GB
OmniStackVC-10-0-2-9	controlador hyperconvergencia	Encendido	Normal	210,04 GB	20,12 GB	108,37 GB
ServHopex	Servidor aplicación Hopex	Encendido	Normal	365,08 GB	145,59 GB	16,1 GB
VeeamProxy01_rep	Servidor respaldos	Encendido	Normal	77,42 GB	16,34 GB	11,98 GB
VM004-ERP-App	Servidor aplicación ERP	Encendido	Normal	255,28 GB	142,52 GB	16,09 GB
VM004-ERP-App-QA1	Servidor aplicación ERP	Encendido	Normal	147 GB	108,6 GB	16,06 GB
VM005-FileServer	Servidor de archivos	Encendido	Normal	1,2 TB	825,58 GB	2,04 GB
VM006-GLPI	Servidor aplicación GLPI	Encendido	Normal	120 GB	43,6 GB	7,97 GB
VM0066-BHRS2	Servidor de respaldos	Encendido	Normal	100 GB	49,91 GB	8,07 GB
VM007-CuentasClaras 2011	Servidor cuentas claras antiguo	Encendido	Normal	724,24 GB	358,92 GB	16,07 GB

VM007-Kali	Servidor Seguridad Kali	Encendido	Normal	200,01 GB	113,15 GB	8,06 GB
VM008-PortalCapacitaciones	Portal capacitaciones QA	Encendido	Normal	239,41 GB	57,07 GB	8,05 GB
VM008-PortalesWeb	Portales web CNE	Encendido	Normal	530,23 GB	247,6 GB	24,12 GB
VM009-MySQL	Base de datos Mysql	Encendido	Normal	105 GB	36,02 GB	8,06 GB
VM011-ERP-BaseDatos	Base de datos ERP	Encendido	Normal	1,08 TB	551,57 GB	16,09 GB
VM012-cabildos	Aplicación cabildos	Encendido	Normal	532,34 GB	36,16 GB	8,06 GB
VM013-Mail	Mail proxy	Encendido	Normal	550,09 GB	34,11 GB	5,79 GB
VM014-Postgresql	Base de datos PostgreSQL	Encendido	Normal	600,09 GB	389,67 GB	16,1 GB
VM015-EPX-app	Servidor EPX	Encendido	Normal	1,22 TB	963,71 GB	16,09 GB
VM016-Encuestas ciudadanas	Servidor Encuestas ciudadanas	Encendido	Normal	280,86 GB	38,05 GB	8,06 GB
VM017-EspaciosPublicitarios	Servidor aplicación Espacios publicitarios	Encendido	Normal	255,07 GB	22,03 GB	8,06 GB
VM018-Intranet	Servidor Intranet	Apagado	Normal	513,55 GB	25,69 GB	0 B
VM019-Moodle-dlm	Servidor Moodle LMS	Encendido	Normal	505 GB	24,09 GB	7,05 GB
VM020-SQL-EPX	Base de datos EPX	Encendido	Normal	652,49 GB	360,86 GB	14,77 GB
VM021-Relatorias	Aplicación Relatorías	Encendido	Normal	510,09 GB	243,49 GB	8,06 GB
VM022-RUPYM	Aplicación Rupym	Encendido	Normal	1,8 TB	842,5 GB	16,09 GB
VM023-delegados	Aplicación delegados	Encendido	Advertencia	510 GB	19,23 GB	8,06 GB
VM024-Estatuto	Aplicación estatuto oposición	Encendido	Normal	510 GB	22,83 GB	8,07 GB
VM025-Trashumancia-Laravel	Aplicación Trashumancia Framework Laravel	Encendido	Normal	563,15 GB	61,25 GB	8,06 GB
VM026-Tribunales	Aplicación Tribunales	Encendido	Normal	510 GB	19,15 GB	8,06 GB
VM027-Veedurias	Aplicación Veedurias	Encendido	Normal	510 GB	18,93 GB	8,06 GB
VM028-SQL-PRD-hopex	Aplicación Hopex	Encendido	Normal	200 GB	64,32 GB	8,07 GB
VM028-URIEL	Servidor Aplicación Uriel	Encendido	Normal	510 GB	18,8 GB	8,06 GB
VM030-Escrutinio-Mesa Escrutinio	Servidor Aplicación	Encendido	Normal	2,15 TB	754,27 GB	9,78 GB

VM031-EscrutiniomesaBaseDatos	Servidor base de datos Escrutinio	Encendido	Normal	420 GB	225,92 GB	3,51 GB
VM032-Centralizador	Servidor aplicación centralizador	Encendido	Normal	260,09 GB	17,14 GB	8,06 GB

4.1.1. Descripción del Servicio

El servicio de replicación de infraestructura debe garantizar la alta disponibilidad, continuidad operativa y protección de la información crítica del Consejo Nacional Electoral (CNE). Para ello, la infraestructura debe estar diseñada con un modelo de redundancia y recuperación ante desastres que permita la operación ininterrumpida de los sistemas críticos.

El proveedor deberá garantizar que toda la infraestructura esté alojada en un DataCenter con certificación mínimo Tier III, del Uptime Institute, y ubicado en Colombia, asegurando latencia mínima y mayor disponibilidad del servicio.

4.1.2. Requisitos Técnicos

- Replicación en Tiempo Real: Sincronización con la infraestructura de respaldo en las instalaciones del CNE en modalidad ActivoPasivo.
- Firewall Avanzado: Filtrado de paquetes, configuración de puertos y reglas UTM con capacidad para SD-WAN.
- Soporte 7x24x365: Atención inmediata para requerimientos críticos.
- Tiempo de Implementación: La réplica deberá estar operativa en un mínimo se otorgará 10 días hábiles para la migración de datacenter y 10 días hábiles adicionales para la configuración del escenario de réplica, lo que otorga en su totalidad 20 días hábiles de trabajo para la implementación total de la solución.
- Prevención de Caídas: Detección de usabilidad en servidores mediante monitoreo de uso de CPU, memoria y almacenamiento.

4.1.3. Especificaciones Técnicas de Cómputo

La solución debe cumplir con los siguientes requerimientos:

- Infraestructura Hiperconvergente con capacidad de respaldo.
- Procesamiento: Deben ser mínimo 64 cores a 2.4 GHz o superior.
- Memoria RAM: 1 TB distribuible entre los servidores virtuales.
- Almacenamiento:
    - 20 TB en discos de estado sólido (SSD) con hotswap.
    - Capacidad de crecimiento a 25 TB bajo demanda.

4.1.4. Línea Base de Infraestructura a Replicar

El servicio debe incluir la replicación de la siguiente infraestructura del CNE:

- Servidores de Aplicaciones y Bases de Datos
- Control centralizado de usuarios.
- Aplicaciones misionales como RUPYM, Relatoría, Trashumancia, Veedurías, Estatuto de la Oposición, etc. o Sistemas de gestión documental y ERP. o Bases de datos SQL Server y PostgreSQL.
- Portales Web
    - www.cne.gov.co
    - rup.cne.gov.co
    - relatorias.cne.gov.co
    - epx.cne.gov.co
    - erp.cne.gov.co
    - Odin.cne.gov.co
    - app.cne.gov.co
    - cnecuentasclaras.gov.co
    - misionales.cne.gov.co
    - integrador.cne.gov.co

4.2. Servicio de Colocation

El servicio de colocation debe permitir el alojamiento de la infraestructura física del CNE en un Rack de 42U, en diferente DC, con un consumo eléctrico de 8KVA cada uno, asegurando redundancia, disponibilidad y escalabilidad.

4.2.1. Equipos que colocar en el DataCenter

Equipo	Cantidad
Servidores Dell PowerEdge	6
Switches 3COM	2
Switches Cisco Catalyst 9300L	2
Hiperconvergencia HP Simplivity	3 nodos
Firewall Fortinet 400E	1
Fortinet FortiSwitch 1048E	2

4.2.2. Sistemas Operativos y Motores de Bases de Datos

El servicio deberá soportar los siguientes sistemas operativos y bases de datos:

- Linux: RHEL 6.8+, CentOS 6.5+, Ubuntu Server 18.04+, Debian 8.0+.
- Windows Server 2019 o superior.

- Motores de Base de Datos: SQL Enterprise 2022 con soporte de fábrica, PostgreSQL.

4.3. Comunicaciones y Redes

La infraestructura debe contar con alta disponibilidad y redundancia en la interconectividad del CNE, asegurando la continuidad operativa y la interconexión eficiente entre sedes.

4.3.1. Características de Red

- Creación de Redes Virtuales:
  - Configuración de subredes, tablas de enrutamiento, VPN, NAT, routing Gateway, DHCP.
- Personalización de Puertos y Protocolos mediante reglas explícitas.
- Direcciones IP Públicas: Mínimo 10 asignables para servicios del CNE.
- Conectividad VPN con IPSec: Acceso seguro y segmentación de tráfico.

4.3.2. Recursos en DataCenter (ACTUAL CNE)

- Alta Disponibilidad en Infraestructura:
  - Servidores (dos (2) simplivity con una cantidad total de 64 cores, 16 socket por equipo)
  - Firewall (Actualmente se tienen 3 FW) o Balanceadores (administrador de un balanceador), o Equipos de Red (administración de Switches).
- Transferencia de Datos: 100 Gbps/mes en el entorno de producción.
- Almacenamiento en Discos SSD con redundancia y replicación. □ Disponibilidad mínima garantizada: 99.95%.

4.3.3. Interconexión entre Sedes

El proveedor deberá garantizar la interconexión segura y eficiente entre las sedes del CNE, con los siguientes requerimientos mínimos:

Canales de Internet:

- Dos canales de 500M en la sede San Martin, en configuración HA
- Dos canales de 100M en la sede San Martin, configurados en modo activo-activo.
- Un canal de 100M en la sede cll 26
- Dos canales de 100M en el DC donde se preste el servicio de colocation
- Un canal de 100M en la nube privada dónde se repliquen los las máquinas virtuales en ambiente productivo.

Canales de datos (MPLS):

- Un canal de 200M entre San Martin y la Registraduría o Un canal de 300M entre San Martin y el DC donde se entregue el servicio de colocation
- Un canal de 100M entre San Martin y la nube privada dónde se repliquen las máquinas virtuales en ambiente productivo
- Un canal de 100M entre el DC donde se entregue el servicio de colocation y la nube privada dónde se repliquen los las máquinas virtuales en ambiente productivo

4.3.4. Gestión de Tráfico y Balanceo

El servicio debe configurar una red SD-WAN que permita:

- Administración centralizada del tráfico entre todas las sedes. □ Balanceo automático de carga y optimización de tráfico.
- Reducción de latencia y priorización de aplicaciones críticas.

4.4. Ciberseguridad

Se debe hacer suministro de los siguientes equipos con un plazo no mayor a 45 dias.

P/N	DESCRIPCIÓN	QTY
FG-401F	18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, 8 x 10GE SFP+ slots, SPU NP7 and CP9 hardware accelerated, 960GB onboard SSD storage, dual AC power supplies	2
FC-10-0401F-809-02-DD	Enterprise Protection (IPS, AI-based Inline Malware Prevention, Inline CASB Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium)	2
FC-10-FD4H1-204-02-DD	Upgrade FortiCare Premium to Elite (Require FortiCare Premium)	2
FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range 300m, LC connector, MMF, 850nm, 0°C to 70°C, for systems with SFP+ slots	12
P/N	DESCRIPCIÓN	QTY
FG-90G	8 x GE RJ45 ports, 2 x 10GE RJ45/SFP+ shared media WAN ports.	1
FC-10-0090G-809-02-DD	Enterprise Protection (IPS, AI-based Inline Malware Prevention, Inline CASB Database, DLP, App Control, Adv Malware Protection, URL/DNS/Video Filtering, Anti-spam, Attack Surface Security, Converter Svc, FortiCare Premium)	1

FC2-10-FECLD-423-02-DD	FortiMail Cloud - Gateway Premium w. Cloud Email API connector support for Microsoft 365, Exchange or Google (101-1000 mailboxes). FortiCare Premium Support included.	550

4.5. Consideraciones Finales

- Garantizar la operación ininterrumpida de los sistemas del CNE.
- Infraestructura 100% redundante y escalable con soporte TIER IV.
- Plazo de implementación: Máximo 15 días calendario.
- Soporte 7x24x365 con tiempos de respuesta inmediatos.
- Disponibilidad mínima del servicio: 99.95%.

---

5. MESA DE AYUDA

Se requiere poner a disposición un equipo humano para atender solicitudes de soporte tecnológico y dudas sobre la operación del servicio. Este equipo debe estar conformado por el siguiente personal:

PERSONAL REQUERIDO PARA MESA DE AYUDA	CANTIDAD
Gerente de proyectos	1
Coordinador de Mesa de servicio	1
Técnico soporte remoto nivel 2	3
Técnico soporte en sitio nivel 1	2
Líder de servicios de infraestructura	1
Especialista en redes y seguridad	1
Desarrollador PHP, Laravel	1
Líder de mesa de servicios	1

5.1. Obligaciones específicas:

1. Proveer a la Entidad a través de la mesa de ayuda, un punto único de contacto (línea telefónica, correo electrónico, mensajería instantánea) mediante el cual se resuelvan y se canalicen todas las necesidades de soporte técnico, funcional y operativo, relativas al uso de los recursos y servicios de la infraestructura tecnológica del CNE.

2. Atender y registrar los números de caso y/o tickets referentes a problemas técnicos o funcionales, indicando el estado de la solicitud, el tiempo de respuesta y la solución implementada.

3. Mantener la comunicación con usuarios finales y responder de una manera oportuna, eficiente y con alta calidad las solicitudes, incidentes, eventos y problemas de servicios de Tecnología de la Información (TI) que se presenten y que impacten la continuidad de la operación (hardware y software) durante la ejecución del convenio

4. Priorizar las solicitudes de acuerdo con su impacto y urgencia.

5. Establecer metodologías y controles idóneos para la correcta prestación del servicio de mesa de ayuda.

6. Garantizar soluciones eficientes en la prestación del servicio y ejecutar los procedimientos necesarios para la atención oportuna del servicio y gestionar las solicitudes reportadas por el usuario final.

5.2. Reportes:

1. Los reportes a la supervisión serán entregados una vez al mes y se deben incluir como mínimo:
    a. Cantidad de incidentes registrados y repetidos
    b. Tiempo de resolución de incidente
    c. Cantidad de incidentes por problema
    d. Tiempo hasta la identificación del problema
    e. Cuantos tickets de cada tipo de servicio hubo
    f. Estadísticas de la cantidad total de tickets del mes/periodo, cuales están resueltos, cuantos pendientes y el estatus de cada uno.
    g. Realizar informes de la operación.
    h. Reportes de los requerimientos, incidentes y problemas presentados en la plataforma, así como las soluciones que surjan en la atención a los usuarios para alimentar la base de conocimiento.
    i. Métricas de cumplimiento y registro de las diferentes actividades que se realicen durante la ejecución del convenio.

5.3. Tiempo de Atención a Fallas

Los incidentes generados y reportados desde la mesa de servicio van a contener la siguiente información:

- Descripción de la falla
- Hora en que se recibe el reporte e incidencia
- Hora en que se atendió el reporte
- Descripción de la solución brindada
- Hora en que se soluciona el reporte o falla

- Seguimiento al análisis de causa raíz

Se debe cumplir con los siguientes niveles de atención:

Prioridad	Tiempo máximo de atención
Urgente	1 hora
Alta	1 hora
Media	2 horas
Baja	4 horas

6. GARANTÍA DE CONTINUIDAD DEL SERVICIO

Con el propósito de garantizar la continuidad y calidad en la prestación de los servicios contratados por el Consejo Nacional Electoral (CNE) de Colombia, el proponente adjudicatario deberá asegurar que la transición entre el proveedor actual y el nuevo proveedor se realice de manera transparente, sin generar interrupciones que afecten la operación de la entidad. Para tal fin, se establecen las siguientes condiciones obligatorias:

6.1. Transición sin Costo para el CNE:

El nuevo proveedor deberá asumir, a su propio costo y sin que ello represente erogación alguna para el CNE, todas las actividades necesarias para garantizar la correcta transición y puesta en marcha de los servicios contratados. Este proceso deberá llevarse a cabo en el periodo comprendido entre la fecha de adjudicación y el inicio efectivo de la prestación de los servicios.

6.2. Plan de Transición Detallado:

El proponente deberá incluir en su propuesta un Plan de Transición que contenga:

- Cronograma de actividades con fechas clave desde la adjudicación hasta la entrada en operación.
- Estrategias para la mitigación de riesgos durante el cambio de proveedor.
- Mecanismos para garantizar la continuidad operativa y la no afectación de los servicios en curso.
- Asignación de personal calificado encargado de la ejecución de la transición.
- Estrategia de comunicación y coordinación con el contratista saliente.

6.3. Servicios Cubiertos por la Transición:

La transición deberá garantizar la continuidad y adecuada prestación de los siguientes servicios que son objeto de contratación:

1. Servicio de Respaldo y Restauración:
    - Gestión y administración de respaldos con capacidad mínima de 150 TB.
    - Respaldo y recuperación de la infraestructura tecnológica, incluyendo servidores, bases de datos y aplicativos misionales.
    - Implementación de políticas de retención y recuperación de información.
2. Servicio de Seguridad para la Protección de Aplicativos y Sistemas:
    - Monitoreo continuo de seguridad (7x24) y respuesta a incidentes. Implementación y gestión de firewalls perimetrales y de aplicaciones (WAF).
    - Análisis de vulnerabilidades y pruebas de penetración (Ethical Hacking). o Detección, prevención y mitigación de amenazas cibernéticas.
3. Servicio de Monitoreo de Seguridad y Análisis de Vulnerabilidades:
    - Supervisión de desempeño y disponibilidad de la infraestructura tecnológica.
    - Escaneo periódico de vulnerabilidades en servidores, redes y aplicaciones.
    - Generación de informes de hallazgos, recomendaciones y planes de remediación.
4. Servicio de Replicación, Colocation y Comunicaciones de Infraestructura:
    - Replicación de 40 máquinas virtuales y sistemas críticos en Data Center.
    - Implementación y operación de servicios de colocation para la infraestructura física del CNE.
    - Garantía de conectividad segura, estable y redundante entre las sedes del CNE.

6.4. Mesa de Ayuda:

- Atención de incidentes, solicitudes y requerimientos operativos bajo un esquema 7x24.
- Gestión de tickets con métricas de cumplimiento y tiempos de atención establecidos.
- Soporte remoto y en sitio con personal especializado en infraestructura, redes y aplicaciones.

6.5. Condiciones sobre la Infraestructura Existente:

- Propiedad de los Elementos Actuales: Se deja constancia de que la infraestructura, hardware, software y demás elementos actualmente utilizados para la prestación de los servicios son de propiedad exclusiva del proveedor saliente. No existe acuerdo de transferencia de dichos elementos al nuevo proveedor, por lo que este deberá emplear sus propios recursos para la implementación y prestación de los servicios.
- No Dependencia de Recursos del Proveedor Saliente: El nuevo proveedor deberá garantizar que la continuidad del servicio no dependa de los elementos, plataformas o recursos que pertenecen al contratista saliente.

6.6. Acceso a la Información Histórica: El proponente será responsable de coordinar con el proveedor saliente la entrega y migración de la información histórica correspondiente al último año, asegurando la integridad, confidencialidad y disponibilidad de los datos durante el proceso de transición.Garantía de Continuidad Operativa:

- El proponente deberá garantizar que, a la fecha de inicio de la prestación de los servicios, todas las plataformas, soluciones y equipos estén operativos y en pleno funcionamiento.
- Se deberán prever mecanismos de contingencia para responder ante cualquier eventualidad que pueda afectar la continuidad de los servicios.
- La entidad no admitirá periodos de interrupción; cualquier afectación a la operación será responsabilidad directa del contratista.

6.7. Compromiso de No Afectación:

El proponente deberá incluir en su oferta una declaración expresa en la que se comprometa a:

- No generar afectaciones operativas al CNE durante la transición.
- Asumir todas las responsabilidades derivadas de un mal proceso de transición.
- Responder por los daños y perjuicios que se puedan generar en caso de incumplimiento de las obligaciones establecidas en esta sección.

6.8. Supervisión y Seguimiento:

- El CNE designará un equipo de supervisión que hará seguimiento al cumplimiento del plan de transición.
- El proponente deberá atender los requerimientos y observaciones realizados por el equipo de supervisión durante el proceso.
- Se deberá presentar un informe semanal de avance de las actividades hasta la entrada en operación de los servicios.

6.9. Acuerdo Complementario:

Como parte integral del presente contrato, se deberá suscribir un Acuerdo de Coordinación para la Transición de Servicios entre el contratista entrante, el contratista saliente y el CNE. Dicho acuerdo deberá contemplar:

- Las actividades y plazos para la entrega de información y documentación.
- Los mecanismos de validación y aceptación de la información migrada.
- La responsabilidad de cada parte durante la ejecución de la transición.

Estas disposiciones buscan asegurar que el cambio de proveedor se realice de forma ordenada, eficiente y sin que se presenten inconvenientes que afecten la operación misional del Consejo Nacional Electoral (CNE).

7. ANS

Con el fin de garantizar la correcta prestación de los servicios descritos en el ANEXO

TECNICO, estos se ejecutarán de acuerdo con la siguiente tabla de ANS en la cual se plasman las fórmulas de medición y los porcentajes de descuento establecidos de acuerdo con el porcentaje de cumplimiento establecido.

ANEXO - ANS (Acuerdo de Niveles de Servicio)

Con el fin de garantizar la correcta prestación de los servicios descritos en el ANEXO TECNICO, estos se ejecutarán descuerdo con la siguiente tabla de ANS en la cual se plasman las fórmulas de medición y los porcentajes de descuento establecidos de acuerdo con el porcentaje de cumplimiento establecido.

Servicio	Descripción	Factor de Medición	Penalidad, Compensación
Respaldo y restauración de información	Hace referencia a la cantidad de respaldos realizados en el perido	Numero de respaldos realizados ---------- 100 Número total de respaldos solicitados	95% a 90% de cumplimiento, descuento de 2% sobre el valor mensual del servicio 89% a 80% de cumplimiento, descuento de 5% sobre el valor mensual del servicio >79% de cumplimiento, descuento de 10% sobre el valor mensual del servicio
Capacidad de almacenamiento 150 TB con redundancia geográfica	Mide la disponibilidad del servicio de almacenamiento externo.	Número de Horas servicio disponible - ---------- 100 Número de horas mes	95% a 90% de cumplimiento, descuento de 2% sobre el valor mensual del servicio 89% a 80% de cumplimiento, descuento de 5% sobre el valor mensual del servicio >79% de cumplimiento, descuento de 10% sobre el valor mensual del servicio
Servicio de Firewall para aplicaciones WAF (configuración, despliegue de políticas y despliegue de registros DNS) ,	Mide el tiempo disponible del servicio protección de aplicaciones WAF	Número de Horas servicio disponible - ----------100 Número de horas mes	95% a 90% de cumplimiento, descuento de 2% sobre el valor mensual del servicio 89% a 80% de cumplimiento, descuento de 5% sobre el valor mensual del servicio >79% de cumplimiento, descuento de 10% sobre el valor mensual del servicio
Servicio de alerta proactiva para la detección de tráfico malicioso y/o ips de reputación en lista negra,	Hace referencia a el número de alertas críticas que se reportan al cliente mediante medios oficiales	Numero alertas criticas reportadas - ----------100 Número alertas criticas detectadas	95% a 90% de cumplimiento, descuento de 2% sobre el valor mensual del servicio 89% a 80% de cumplimiento, descuento de 5% sobre el valor mensual del servicio >79% de cumplimiento, descuento de 10% sobre el valor mensual del servicio
Escaneo y monitoreo de vulnerabilidades en servidores,	Mide la cantidad de servidores analizados en busca de vulnerabilidades	Numero de servidores analizados al mes - ---------- 100 Número total de servidores objeto de análisis	95% a 90% de cumplimiento, descuento de 2% sobre el valor mensual del servicio 89% a 80% de cumplimiento, descuento de 5% sobre el valor mensual del servicio >79% de cumplimiento, descuento de 10% sobre el valor mensual del servicio

Monitoreo y análisis de y rendimiento de consumo por recursos parte de servidores virtuales y físicos,	Mide la cantidad de servidores monitoreados para establecer patrones de uso de recursos de hardware	Numero de servidores analizados al mes - ---------- 100 Número total de servidores objeto de análisis	95% a 90% de cumplimiento, descuento de 2% sobre el valor mensual del servicio 89% a 80% de cumplimiento, descuento de 5% sobre el valor mensual del servicio >79% de cumplimiento, descuento de 10% sobre el valor mensual del servicio
Servicio de interconexión entre sedes	Mide la disponibilidad de los canales de datos e internet	Número de Horas servicio disponible - ---------- 100 Número de horas mes	95% a 90% de cumplimiento, descuento de 2% sobre el valor mensual del servicio 89% a 80% de cumplimiento, descuento de 5% sobre el valor mensual del servicio >79% de cumplimiento, descuento de 10% sobre el valor mensual del servicio
Replicación Infraestructura crítica,	Mide la disponibilidad y acceso a los servidores replicados	Número de Horas servicio disponible - ---------- 100 Número de horas mes	95% a 90% de cumplimiento, descuento de 2% sobre el valor mensual del servicio 89% a 80% de cumplimiento, descuento de 5% sobre el valor mensual del servicio >79% de cumplimiento, descuento de 10% sobre el valor mensual del servicio
Servicio Colocation infraestructura física,	Disponibilidad de servidores físicos en datacenter remoto	Número de Horas servicio disponible - ---------- 100 Número de horas mes	95% a 90% de cumplimiento, descuento de 2% sobre el valor mensual del servicio 89% a 80% de cumplimiento, descuento de 5% sobre el valor mensual del servicio >79% de cumplimiento, descuento de 10% sobre el valor mensual del servicio
MESA DE AYUDA,	Mide la cantidad de Tikets resueltos dentro de los tiempos establecidos de acuerdo con su criticidad	Numero de tikets resueltos dentro de los tiempos - ---------- 100 Número total de tikets reportados	95% a 90% de cumplimiento, descuento de 2% sobre el valor mensual del servicio 89% a 80% de cumplimiento, descuento de 5% sobre el valor mensual del servicio >79% de cumplimiento, descuento de 10% sobre el valor mensual del servicio