Tabla de contenido

REQUERIMIENTOS GENERALES 5

1. SOLUCIÓN DE INFRAESTRUCTURA EN SITIO ALTERNO PARA REDUNDACIA 5

Descripción General del Servicio 5

Infraestructura y Componentes a Respaldar en sitio alterno 5

Características de almacenamiento de propósito específico para Backup. 6

Frecuencia de Respaldo 7

Requisitos del Almacenamiento de Respaldo 7

Conectividad 7

Soporte e implementación 8

Identificación y Documentación de los Respaldos 8

Entrega y Administración de la Información 8

Requisitos de Personal y Supervisión 8

Consideraciones Finales 9

Características de nodos de procesamiento para sitio alterno DRP 9

Características técnicas de la solución 9

Especificaciones técnicas del bien o servicio HCI 9

Especificaciones técnicas del bien o servicio SWITCHES TOR 17

Especificaciones técnicas del bien o servicio GESTOR DE BACKUP 18

Respaldo en nube y restauración con capacidad de 150 TB 19

Tipos de Respaldo 19

Requisitos de Disponibilidad y Recuperación 20

Requisitos de Software y Seguridad 20

2. SERVICIO DE SEGURIDAD PARA LA PROTECCIÓN DE LOS APLICATIVOS DEL CNE ... 20

Descripción General 20

Alcance del Servicio 20

Controles de Seguridad en la Infraestructura 21

Monitoreo y Respuesta ante Incidentes 22

Evaluación de Seguridad y Protección Perimetral 22

Seguridad de Redes y Protección contra Amenazas Externas 22
Servicio de Firewall para Aplicaciones Web 22
Características y Funcionalidades 22
Mecanismos de Protección y Detección de Amenazas 24
Servicio DDoS (Denegación de Servicio Distribuido). 25
Ethical Hacking y Pruebas de Seguridad 26
Entregables y Reportes 26
Reportes de Seguridad 26
Requisitos de Cumplimiento y Normatividad 27
Consideraciones Finales 27
3. SERVICIO DE ANÁLISIS DE DISPONIBILIDAD, SEGURIDAD Y VULNERABILIDADES 27
Descripción General 27
Monitoreo de Desempeño, Seguridad y Disponibilidad 28
Acceso y Configuración del Sistema de Monitoreo 28
Despliegue del Agente de Monitoreo 29
Operación del Sistema de Monitoreo 29
Servicio de Análisis de Vulnerabilidades 32
Alcance del Escaneo de Vulnerabilidades 32
Frecuencia y Ejecución del Escaneo 33
Reportes y Entregables 33
Requisitos de Seguridad y Cumplimiento 33
Consideraciones Finales 34
4. SERVICIO DE REPLICACIÓN, COLOCATION Y COMUNICACIONES DE INFRAESTRUCTURA TECNOLÓGICA DEL CNE MISION CRITICA. 34
Replicación de Infraestructura Crítica 34
Descripción del Servicio 35
Requisitos Técnicos 35
Línea Base de Infraestructura a Replicar 36
Servicio de Colocation 36
Equipos que colocar en el Datacenter Principal 36

Equipos que colocar en el Datacenter Alterno 37
Comunicaciones y Redes 37
Características de Red 37
Recursos en DataCenter (ACTUAL CNE) 37
Interconexión entre Sedes 37
Gestión de Tráfico y Balanceo 38
Consideraciones Finales 38
5. MESA DE AYUDA 38
Obligaciones específicas: 39
Reportes: 40
Tiempo de Atención a Fallas 40
6. SOLUCIONES DE CIBERSEGURIDAD 41
Control De Acceso A La Red (NAC) 41
Solución DLP (Data Loss Prevention) 45
Sistema de control de acceso con reconocimiento facial. 51
SUMINISTRO TERMINALES DE RECONOCIMIENTO FACIAL (CAPACIDAD 2800 ROSTROS) ... 53
Protección de correo electrónico. 54
7. SALAS DE VIDEO CONFERENCIA 58
Visualización (Pantalla) 59
Captura de Video (Sistema Dual de Cámaras) 59
Audio (Micrófonos de Mesa) 59
Procesamiento y Grabación (Hub Central) 59
Instalación y Puesta en Marcha 60
8. GARANTÍA DE CONTINUIDAD DEL SERVICIO 60
Transición sin Costo para el CNE: 60
Plan de Transición Detallado: 60
Servicios Cubiertos por la Transición: 61
Mesa de Ayuda: 61
Condiciones sobre la Infraestructura Existente: 61
Garantía de Continuidad Operativa: 62

Compromiso de No Afectación: 62

Supervisión y Seguimiento: 62

Acuerdo Complementario: .....**¡Error! Marcador no definido.**

9. ANS 62

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, disponibilidad y mecanismos de recuperación ante desastres y redundancia en sitios alternativos de los distintos softwares que soportan los aplicativos misionales del CNE

REQUERIMIENTOS GENERALES

1. SOLUCIÓN DE INFRAESTRUCTURA EN SITIO ALTERNO PARA REDUNDACIA

Descripción General del Servicio

La entidad en su plan de fortalecimiento de las capacidades de infraestructura tecnológica adquirió un sistema de nodos de procesamiento y almacenamiento con redundante N+1, y un sistema de propósito específico para Backup, el cual está alojado en el Datacenter principal de CNE, en aras de garantizar una continuidad operativa y de servicio la entidad está en el propósito de implementar un mecanismos de recuperación ante desastres y redundancia en sitio alterno, por lo cual requiere adquirir e implementar una solución de Backup que replique las capacidades alojadas en el sistema actual de nodos de procesamiento, así como también toda la información del sistema de almacenamiento de propósito específico para Backup, en una infraestructura alojada en Datacenter alterno con el propósito de tener un punto de restauración para recuperación ante incidentes.

La solución de respaldo 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 ante desastres conforme a las políticas establecidas.

Infraestructura y Componentes a Respaldar en sitio alterno

El sistema de respaldo ante desastres deberá contar con capacidades para soportar y garantizar la protección y replicación de la siguiente infraestructura de misión crítica de la entidad:

VM	CPUs	Memory	Disks	Total, disk capacity MiB
VM004	6	16.384	2	150.528
VM005	1	2.048	3	1.261.568
VM007	8	16.384	3	741.376

VM008	8	24.576	3	542.720
VM009	4	8.192	1	107.520
VM011	8	16.384	5	642.048
VM014	16	16.384	1	614.400
VM018	4	8.192	2	517.120
VM020	4	16.384	6	667.648
VM021	4	8.192	1	522.240
VM022	8	16.384	2	1.044.480
VM028	4	8.192	1	204.800
VM032	4	8.192	1	266.240
VM034	8	16.384	6	2.191.360
VM043	4	8.192	1	204.800
VM044	4	8.192	1	256.000
VM053	4	8.192	1	153.600
VM056	2	8.192	1	204.800
VM058	4	8.192	1	204.800
VM065	4	8.192	1	204.800
VM070	4	16.384	1	204.800
VM071	4	32.768	2	512.000

Características de almacenamiento de propósito específico para Backup.

La solución deberá tener la capacidad de integrarse con el sistema actual de la entidad (Ex189-sec) de manera nativa y de construir un sistema de almacenamiento para backup en arquitectura scale-out que le permita tener a la entidad una solución de disaster recovery.

Como requisitos indispensables del sistema de almacenamiento de propósito específico para Backup del sitio alterno deberá cumplir con los siguientes puntos técnicos:

- Mínimo 1 nodo o equipo de almacenamiento de propósito específico para Backup, que será el sistema de recuperación ante desastres del sistema de almacenamiento actual Ex189-sec, este deberá integrarse de manera nativa con el sistema actual instalado en la entidad en sitio principal.
- Este sistema le debe permitir a la entidad seguir creciendo en mínimo 12 nodos de diferente modelo y capacidad
- Deberá soportar Integración completa con el actual sistema scale-out de la entidad y construir una arquitectura para recuperación de desastre soportando la replicación de la solución actual del CNE.
- Debe soportar replicación de ExaGrid (solución implementada actualmente en sitio principal) con deduplicación y cifrado.
- Debe administrarse por la misma consola del sistema de almacenamiento actual de exagrid, basado en https con certificados TLS, permitiendo separar o filtrar los tráficos para los respaldos de los de administración en cada una de las interfaces de red.

- Debe soportar la replicación de los datos de backup con eficiencia de ancho de banda de hasta 25:1.
- La solución final con el ambiente actual más el o los equipos propuestos deben soportar replicación cifrada 256-bit AES de exagrid.
- Debe soportar doble factor de autenticación, para usuarios locales e integración con directorio activo.
- Debe soportar integración con Veeam Backup and Replication, software de respaldo actual de la entidad usando Veeam Data Mover y S3 en el propio equipo propuesto.
- Debe incluir alertas o alarmas ante posibles cifrados en el almacenamiento principal o el mismo sistema de almacenamiento para backups.
- Debe detectar automáticamente, alertar y proteger ante posibles ataques maliciosos que puedan destruir los respaldos con estrategias de borrado.

Nota: Toda referencia a marca, fabricante o tecnología se entenderá como parámetro técnico referencial, aceptándose soluciones equivalentes o superiores, siempre y cuando lo ofertado mantenga un 100% de compatibilidad de manera nativa (sin instalación de parches o desarrollos) con la infraestructura existente en el CNE.

Frecuencia de Respaldo

- Respaldos incrementales diarios
- Almacenamiento de respaldos offsite en una ubicación externa segura para la protección ante desastres.

Requisitos del Almacenamiento de Respaldo

El sistema de respaldo debe soportar un almacenamiento con capacidad RAW 212 TB, y una capacidad usable de 162TB, permitiendo la protección de los sistemas críticos del CNE, asegurando la continuidad operativa ante fallos, desastres o ataques cibernéticos.

- Capacidad RAW 212TB o superior
- Capacidad Usable de 160TB o superior
- El o los equipos propuestos debe entregar un air-gap e inmutabilidad de los datos para 60TB usables o superior
- Debe permitir al sistema de almacenamiento de la entidad continuar creciendo a mínimo 3PB
- El o los equipos propuestos no deben ocupar más de 2 unidades de rack y en profundidad del rack no debe superar los 90CM o 900mm

Conectividad

- 2 puertos de red de 1GbE

- Mínimo 2 puertos de red SFP+ Optical 10Gbps, estos deben permitir actualizaciones a 25Gbps
- 1 puerto IPMI para administración remota

Soporte e implementación

- La integración del nuevo equipo con los existentes en la entidad lo debe realizar un ingeniero de fabrica
- Todo el sistema se debe entregar actualizado a la última versión de firmware estable conocida y recomendada por el fabricante
- El soporte y mantenimiento debe coincidir con los equipos actuales de la entidad
- Se debe incluir el acompañamiento de un ingeniero del fabricante por el tiempo de soporte contratado, este ingeniero debe implementar con la entidad eventos correctivos, preventivos o derivados de buenas prácticas recomendadas, incluyendo las actualizaciones de la solución
- Debe tener opciones de monitoreo y alertas al fabricante, con el objetivo de agilizar tareas de soporte

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.

Entrega y Administración de la Información

- Se debe proporcionar acceso con rol de administrador global al recurso de almacenamiento a un funcionario designado por el CNE.
- La administración de la solución de respaldos estará alineada a las políticas de respaldo que la supervisión del contrato apruebe.

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 desastres.
- Implementación de alertas tempranas ante posibles fallos en el sistema de respaldo.

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.
- La solución debe estar alineada con los estándares de seguridad y mejores prácticas internacionales en gestión de respaldos.

Características de nodos de procesamiento para sitio alterno DRP

El CNE para garantizar la continuidad de las operaciones requiere adquirir una solución de nodos de procesamiento y almacenamiento con redundancia N+1, como mecanismos de recuperación ante desastres y redundancia en sitio alterno para el consejo nacional electoral, de acuerdo con las especificaciones técnicas del anexo.

Compuestas por las siguientes características técnicas:

Características técnicas de la solución

- Nodos de procesamiento y almacenamiento con redundancia N+1
- Dos (2) Switch LAN de mínimo 24 puertos con interfaces de 10GbE “SFP+” para la conectividad de los Appliances.
- Un (1) Switch LAN de gestión de 1Gb Base-T
- Todos los componentes como patch cord de fibra y ethernet necesarios.
- 14 modulos sfp+
- 2 cables DAC QSFP28

Especificaciones técnicas del bien o servicio

CARACTERISTICAS	REQUERIMIENTOS MINIMOS
Fabricante y modelo	Especificar
Cantidad de clúster	Mínimo 3
ITEM 1	**Solución de** Nodos de procesamiento y almacenamiento con redundancia N+1

Hardware requerido por Appliance	
Características de los Cluster	Los appliances del fabricante del hardware deberá ser reconocida mundialmente, tener respaldo y garantía donde sean instalados, por parte de personal certificado de la maraca. Los appliances ofrecidos deben ser tanto en el portal del fabricante del hardware como appliances o sistemas integrados, integrados y pretesteados desde fábrica, son de propósito específico. Permitir crecimientos heterogéneos, compatibilidades, interoperabilidad y desarrollos de firmware pretesteados para los appliances. Esto deberá certificarse evidenciando los respectivoslinks Como appliances o sistemas integrados deberá proveer punto único de soporte tanto para el hardware por parte del fabricante del appliances o sistema integrado.
Procesadores	La solución de nodos de procesamiento deberá tener por cluster un mínimo de: **Procesadores:** 2 Procesadores de 16 cores, cada uno **Velocidad de reloj:** 3,6 GHz o superior **Tecnología del procesador:** INTEL o AMD de última generación o una generación anterior el cual deberá garantizar el óptimo funcionamiento de la herramienta El clúster de hiperconvergencia ofertado deberá garantizar como mínimo 96 cores físicos distribuidos en un mínimo de tres (3) appliances.
Memoria	La solución de nodos de procesamiento debe contar con memoria RAM de mínimo 1.536 GB (total del clúster) en módulos DDR5 como mínimo La solución deberá contar por nodo con memoria RAM de mínimo 512 GB en módulos DDR5 como mínimo
Capacidad Mínima	La solución de nodos de procesamiento deberá ser conformada con un mínimo de 3 clúster en un nodo para garantizar lo requerido en las especificacionessolicitadas en este documento
Almacenamiento	Para efectos del estudio de mercado los oferentes deben cotizar la siguiente opción con todas las demás características incluidas, Capacidad total por clúster: 26TB efectivos usables Consideraciones: La solución de nodos de procesamiento debe garantizar como mínimo: Tipo de unidades: full NVMe o superior. Capacidad de las unidades: 7 TB por unidad de almacenamiento. Los TB garantizados deben ser antes de compresión, deduplicación o algoritmos de optimización.

Conectividad	Cada clúster deberá contar con mínimo: Dos (2) Puertos 10/25GB SFP28 o SFP+, incluyendo 2 Transceiver SFP+ y fibras respectivas. Cada appliance deberá contar con mínimo uno (1) puertos Ethernet 1GbEBase-T para tráfico de administración.
Puertos USB	Cada appliance deberá contar con mínimo uno (1) puertos USB 3.0.
Generalidades	Los componentes ofertados deben ser nuevos de fábrica, no remanufacturados, ni reparados, ni reacondicionados en ninguna de sus partes.
	Suministrar una solución de nodos de procesamiento cuyo software sea agnóstico y pueda implementarse sobre múltiples fabricantes de hardware en un mismo clúster, así como en nubes públicas como Azure, AWS y Google
	La solución de nodos de procesamiento deberá proveer un crecimiento modular y escalable, garantizando el aprovisionamiento tanto de cómputo, memoria y almacenamiento.
	La solución debe tener la capacidad de crecimientos modulares en el mismoclúster.
	Dada la criticidad de las cargas de la entidad y de la importancia de la soberanía de sus datos a nivel de replicaciones y los planes de recuperación ante desastres, la solución deberá manejar replicación nativa a nivel de hipervisor para la protección de sus cargas descartando el uso de herramientas de terceros que operen mediante agentes externos o proxies adicionales.
	La solución de nodos de procesamiento debe incluir e integrar funcionalidades de aprovisionamiento y monitoreo.
Fuentes de alimentación	Dos (2) fuentes de alimentación AC, Voltaje 200 a 240 VAC, frecuencia 60 HzRedundancia (1 + 1), para cada uno de los appliances de hiperconvergencia Ofertados
Unidad de medida	Cada appliance de los nodos de procesamiento ofertado no debe ser superior a dos (2) unidades de rack.
Características del hipervisor	Debe encontrase como líderes en software de infraestructura de nodos de procesamiento y almacenamiento con redundancia N+1, en el Cuadrante Mágico de gartner en su última publicación.
	La solución debe incluir una arquitectura que provea a nivel de hardware y software un esquema de alta disponibilidad de tal forma que, ante la falla de un appliance, se mantenga operativo el clúster sin afectar el desempeño de las aplicaciones, este esquema puede o no incorporar elementos que hagan la función de testigo, según las mejores prácticas del fabricante.
	Siendo la solución de nodos de procesamiento y almacenamiento con redundancia N+1

	definida por software.
	El hipervisor ofrecido con la solución de nodos de procesamiento y almacenamiento con redundancia N+1, debe contar con la capacidad de ubicación de máquinas virtuales utilizando estadísticas de usode CPU/RAM/almacenamiento del clúster en tiempo real de manera que se garantice a las cargas de trabajo el mejor acceso posible a los recursos. Adicionalmente el hipervisor deberá estar de manera nativa con la herramienta.
	El hipervisor ofrecido con la solución de nodos de procesamiento y almacenamiento con redundancia N+1, debe poder ser actualizado desde la misma consola gestión del sistema hiperconvergente a las últimas versiones sin disrupción del servicio.
Características de los Cluster	La solución propuesta debe incorporar la capa de software de gestión de la infraestructura de nodos de procesamiento y almacenamiento con redundancia N+1 instalada como un servicio en cada unode los cluster que componen la solución manteniendo una arquitectura de alta disponibilidad, garantizando la consistencia y disponibilidad de la información.
	La solución deberá proporcionar un mecanismo de actualización del software de la infraestructura completa del clúster (servicios de storage, componentes de los appliances e hipervisor) directamente desde la consola web y de forma no disruptiva.
	El Hipervisor debe disponer de funcionalidades de alta disponibilidad, balanceo de cargas, modo de mantenimiento, y actualizaciones de software
	La solución debe incluir una arquitectura que provea a nivel de hardware y software un esquema de alta disponibilidad de tal forma que, ante la falla de un appliance, se mantenga operativo el clúster, este esquema puede o no incorporar elementos que hagan la función de testigo de forma nativa (witness, quorum o similar), según las mejores prácticas del fabricante
	Soporte y garantía de toda la solución ofrecida (software y hardware)directamente con el fabricante, a partir de la fecha de entrega de los equipos por: tres (1) años.
Almacenamiento	
	La interfaz de administración de solución de nodos de procesamiento y almacenamiento con redundancia N+1, deberáentregar estadísticas completas sobre las máquinas virtuales como consumos de vCPU, RAM, y discos, así como IOPS de lectura, IOPS de escritura y latencias.
	La interfaz para la administración debe permitir determinar en tiempo real elconsumo de los recursos de CPU, Memoria RAM, y almacenamiento.
	La interfaz deberá permitir gestión global y federada, es decir, desde un solo panel de administración se deberán gestionar todos los componentes de la solución hiperconvergente.

	La interfaz debe soportar la creación de proyectos donde se puedan definirlos recursos y requerimientos que los usuarios puedan tener acceso según su Perfil
CARACTERISTICAS ESPECÍFICAS	
	La solución debe tener la capacidad de crecimientos modulares en el mismo clúster, incrementado el número de servidores; que podrán ser de diferentefamilia y modelo del fabricante, con diferentes capacidades de procesamiento (diferente generación de procesadores), diferente tamaño de memoria
	La solución debe poder ejecutar de-duplicación y **compresión** a lo largo de todo el clúster (de forma global) y no limitadas al contenido de los discos de cada appliance. Las funcionalidades de compresión y de-duplicación deben poder activarse o desactivarse por parte del administrador del sistema ya sea que ambas estén activas o solo una de las dos en el clúster o según las mejores prácticas de cada fabricante.
	Suministrar una solución, compuesta por recursos de cómputo, almacenamiento, gestión centralizada, software de hiperconvergencia de forma integrada homologada y preinstalada de fábrica que aproveche los componentes locales de cada unidad y cree una plataforma distribuida donde todas las funcionalidades estén basadas en el software y no dependan de un componente de hardware específico para su funcionamiento.
	El sistema hiperconvergente debe llevar a cabo las actividades de compresión y/o de-duplicación completamente en software, sin requerir el uso de ningún hardware especializado para esta funcionalidad.
	La solución de nodos de procesamiento y almacenamiento con redundancia N+1 debe soportar protocolos IPV4 e IPV6.
	La solución de nodos de procesamiento y almacenamiento con redundancia N+1 debe incluir compresión, sin licenciamiento adicional.
	La solución debe soportar el respaldo y restauración de copias de las máquinas virtuales y archivos hacia la nube pública.
	La solución debe detectar de manera proactiva el daño de un disco, removerlo de manera lógica automáticamente del clúster y reconstruir de manera inmediata los datos que ahí se alojaban en los otros discos del clúster. En caso, que el disco sea removido o se vaya estado fuera de línea (offline), la reconstrucción de los datos también debe indicarse de manera automática e inmediata.
RÉPLICA	

	La solución debe incluir la funcionalidad de replicación asincrónica nativa de datos, que cumpla con los siguientes requerimientos básicos: Replica a nivel de máquina virtual de forma granular. La réplica a nivel VM Mecanismos de compresión y/o de-duplicación de los datos a ser replicados. Replicación bidireccional entre dos centros de datos. Posibilidad de limitar el ancho de banda usada por la replicación.
Especificaciones complementarias de la solución Hiperconvergente:	
	La interfaz de administración de solución de hiperconvergencia, deberá entregar estadísticas completas sobre las máquinas virtuales como consumos de vCPU, RAM, y discos, así como IOPS de lectura, IOPS de escritura y latencias. Garantía suministrada directamente por el fabricante de la solución de hiperconvergencia para el CNE mínimo por un (1) año. Realizar la entrega de nuevas actualizaciones, sin costo durante el tiempo de garantía mínimo un (1 año) de la licencia (Nuevas versiones, actualizaciones, mejoras y mantenimiento de la licencia del Presente contrato) La solución de hiperconvergencia debe integrar herramientas de monitoreo y análisis predictivo de capacidad de cómputo, que permita determinar el análisis de crecimiento, de acuerdo con las necesidades de la entidad. La interfaz de administración y monitoreo de la solución de Hiperconvergencia deberá proveer accesos alternativos basados en SSH y/o interfaces seriales remotas. La solución debe incluir una arquitectura que provea a nivel de hardware y software un esquema de alta disponibilidad de tal forma que, ante la falla de un clúster, se mantenga operativo el nodo sin afectar el desempeño de las aplicaciones, este esquema puede o no incorporar elementos que hagan la función de testigo (witness, quorum o similar), según las mejores prácticas del fabricante. La solución debe tener la capacidad de crecimientos modulares en el mismo clúster, incrementado el número de servidores; que podrán ser de diferente familia y modelo del fabricante. Capacidades de procesamiento (diferente generación de procesadores), diferente tamaño de memoria y diferente tipo de almacenamiento (clúster con almacenamiento híbrido y/o clúster con almacenamiento solo de estado sólido). La solución debe incluir una funcionalidad que realice detección de anomalías, basadas en análisis de comportamiento para generar alertas tempranas. Las capacidades de procesamiento, detección de anomalías, crecimiento alta disponibilidad solicitadas deberán estar definidas en el datasheet emitido por el fabricante de la solución y se deberán allegar como parte de la propuesta. La solución debe incluir una función que permita al grupo de Sistemas crear tareas

	automatizadas para acciones de remediación o troubleshooting, basadas en alertas a través de un Wizard de Configuración. El Oferente deberá garantizar que todo el software que ponga a disposición del CNE para la prestación del servicio se encuentra debidamente licenciado o suscrito cumpliendo con las políticas de distribución y uso de software del fabricante. El Oferente debe manifestar que acepta que el CNE verifique el licenciamiento del software utilizado. Soportar integración **mediante** el uso de REST API, a otras soluciones de administración para facilitar la integración con ambientes de monitoreos actuales. La interfaz debe permitir la creación de diferentes roles de usuarios. La interfaz debe permitir el análisis de ancho de banda utilizado por la misma, así como el ancho de banda de una máquina virtual
Garantía y servicios para la solución de Hiperconvergencia	
	La infraestructura de almacenamiento y los switches se deben entregar configuradas y en perfecto funcionamiento de acuerdo con las mejoresprácticas que establezca el fabricante. Sin costo adicional para el CNE y por el periodo de la garantía es decir mínimo por un (1) año. El material didáctico e informativo que se proporcione (guías de instalación configuración, manuales, fichas técnicas de los equipos) debe ser como mínimo el material oficial o avalado por el fabricante, así como el adicional quesea requerido para este fin y deberá estar en idioma español y/o inglés y será entera responsabilidad del contratista.
	Atención telefónica 24x7, apertura de casos vía web, correo electrónico o llamada telefónica, interfaz web para seguimiento a los casos de soporte que se generen en la herramienta de Help Desk El oferente deberá contar con una mesa de servicio para apoyo a las solicitudesde soporte realizadas a fábrica. Los requisitos de esta mesa de servicio se establecen en el numeral 5 del presente documento
	El oferente debe garantizar el personal idóneo para la instalación, configuración, migración de datos y puesta en funcionamiento de la solución adquirida. La instalación, configuración y puesta en marcha de la solución de Hiperconvergencia, debe incluir la transferencia de conocimiento y capacitación necesaria para la administración de la totalidad de herramientas que integran la solución de recuperación ante desastres del sistema de hiperconvergencia de hasta 12 horas mínimo para 3 servidores públicos. Esta deberá ser construida y presentada por el contratista, conteniendo los temas necesarios para la apropiación técnica del proyecto y deberá ser aprobada por el supervisor del contrato. Debe ser impartida por personal capacitado y certificado en la solución ofertada de hiperconvergencia, (Certificación Vigente emitida por el fabricante de la solución). Los dispositivos ofertados, deben ser instalados, conectados, configurados d integrados a la plataforma tecnológica de la entidad. Los servicios de instalación, configuración, migración y puesta en operación de la solución de hiperconvergencia ofertados deben ser realizados por el contratista; con personal idóneo

	directo del fabricante y/u oferente. El contratista instalará, configurará, hará las pruebas y entregará en completa operación con todos los elementos necesarios de la solución que garanticen su pleno funcionamiento en un plazo no mayor a 45 días calendario, contados a partir de la firma de acta de inicio. El contratista incluirá sin costos para el CNE todos los servicios necesarios para la instalación, configuración y puesta en delclúster HCI en el sitio alterno que hace parte del DRP. Los servicios de instalación, configuración, migración y capacitación deben ser suministrados por el oferente
Gestión y Monitoreo	La solución deberá permitir gestión global y federada, es decir, desde un solo panel de administración se deberán gestionar todos los componentes de la infraestructura de hiperconvergencia ofertada. Desde una única consola de gestión se tenga visibilidad tanto de los recursos virtuales como de hardware.
	La consola de administración de solución de nodos de procesamiento y almacenamiento con redundancia N+1 ofrecida deberá entregar estadísticas completas de consumos de CPU, RAM, y discos, así como IOPS de lectura, IOPS de escritura y latencias. Esta información debe estar presente en la misma consola de gestión y administración de la solución de HCI.
	El sistema de administración y monitoreo del almacenamiento ofertado deberá proveer accesos alternativos basados en SSH y/o interfacesseriales remotas.
Garantía Servicios	El proponente deberá generar y entregar toda la documentación que requiera el CNE, pero como mínimo la asociada a la definición, diseño, planeación e implementación de la arquitectura para la solución de almacenamiento ofertada.
	Garantía suministrada directamente por el fabricante de la solución de nodos de procesamiento y almacenamiento con redundancia N+1 para el CNE por mínimo un (1) año. Incluye soporte técnico y garantía por mínimo un (1) año.
	Realizar la entrega de nuevas actualizaciones, sin costo durante el tiempode garantía un (1 año) de la licencia (Nuevas versiones, actualizaciones, mejoras y mantenimiento de la licencia del presente contrato) de nodos de procesamiento y almacenamiento con redundancia N+1.
	Los servicios de instalación, configuración, migración y puesta en operación de la solución de almacenamiento ofertados deben ser realizados por el contratista; con personal directo del fabricante, idóneo y experto en soluciones iguales a la ofertada a la entidad.
	El contratista incluirá sin costos para el CNE todos los servicios necesarios para la instalación, configuración y puesta en funcionamiento de los nodos de procesamiento y almacenamiento con redundancia N+1.
	El contratista instalará, configurará, hará las pruebas y entregará en completa operación con todos los elementos necesarios de la solución que garanticen su pleno funcionamiento en un plazo no mayor a 45 días calendario contados a partir de la firma de acta de inicio..

	El Oferente deberá garantizar que todo el software que ponga a disposición del CNE, para la prestación del servicio se encuentra debidamente licenciado o suscrito cumpliendo con las políticas de distribución y uso de software del fabricante.
	El material didáctico e informativo que se proporcione *(guías de instalación y configuración, manuales, fichas técnicas de los equipos)* debe ser como mínimo el material oficial o avalado por el fabricante, así como el adicionalque sea requerido para este fin y deberá estar en idioma español y/o inglés y será entera responsabilidad del contratista.
CERTIFICACIONES DE NODOS DE PROCESAMIENTO Y ALMACENAMIENTO CON REDUNDANCIA N+1:	
	CERTIFICACIÓN DISTRIBUIDOR AUTORIZADO: El proponente debe adjuntar carta del fabricante de los bienes y/o equipos, donde certifique que es distribuidor autorizado en Colombia. donde se acredite estar en la capacidad técnica de configurar, mantener y dar soporte técnico de los equipos. La certificación no debe superar una antigüedad mayor de 30 díashacia atrás desde la fecha del cierre del presente proceso.
	CATÁLOGOS: El proponente debe anexar en la oferta la información que facilite la verificación de los factores técnicos mínimos de obligatorio cumplimiento, tales como fichas de especificaciones técnicas, certificaciones, folletos y todas aquellas que permitan validar características técnicas, por cada elemento ofertado, preferiblemente en idioma español.
	CERTIFICACIÓN EOL DE LOS EQUIPOS OFERTADOS, el oferente deberá aportar certificación emitida por el fabricante de los bienes correspondiente a los bienes objeto del presente proceso de contratación, donde se indique que los equipos ofertados son nuevos, no remanufacturados o reconstruidos, que no se encuentran declarados EOL (END OF LIFE) o fuera de la vida útil. La Certificación debe estar vigente y no debe ser expedida con una antelación superior a treinta 30 días a la fecha de cierre del proceso, además el equipo debe tener no más de 3 años de lanzado en el mercado.
	CERTIFICACIÓN DE DISPONIBILIDAD DE REPUESTOS: Anexar Certificación del fabricante garantizando el suministro y disponibilidad de repuestos necesarios para el correcto funcionamiento delos equipos ofertados durante los siguientes (3) años contados a partir delrecibo a satisfacción de los equipos.

Especificaciones técnicas del bien o servicio SWITCHES TOR

ITEM 2	**SWITCHES LAN**
CARACTERÍSTICAS	**REQUERIMIENTOS MÍNIMOS**
Cantidad	Mínimo dos (2)
Escalabilidad	Capacidad de 24 puertos los cuales deben estar activos.
Capacidad mínima por cada Switch	
	24x 10G/1G SFP+/SFP ports and 2x 100G/40G QSFP28/QSFP+ ports RJ-45 Serial Console Port: 1 10/100/1000 Service Ports: 1

REQUERIMIENTOSMÍNIMOS	Mínimo 880 Gbps de Switching bandwidth Paquetes por segundo (dúplex) a 64 bytes: 1309 Mpps Mac Address: 64.000 VLAN soportadas: 4.000 Memoria: 8GB DDR4 Power Requerido: 100–240V AC, 50–60 Hz Fuente de poder redundante: Doble AC intercambiable en caliente (hot swappable)
	Es requerida la conexión 1/10/Gbps Incluir transceivers y accesorios de red necesarios para la conexión a la red del DRP. entre switch, Incluir los Cables DAC
	La solución de switch se debe poder gestionar por conexión serial a consola,ssh y/o WEB
	Debe incluir los cables (poder, red, fibra óptica, módulos SFP), rieles de montaje y licenciamiento. Y de más elementos que se requieran para que la solución funcione de formaóptima.
	LA solución debe ser interoperable: (Rapid PVST), Spanning Tree Instances (MSTP/CST), Dynamic Routing Protocols (IPv4/IPv6): OSPF, RIP, VRRP, BGP, ISIS
	Deberá incluir las siguientes características: VXLAN L2 and L3 gateways o similar Centralized and distributed gateways o similar BGP Ethernet VPN Enrutamiento (IPv4/IPv6): 8K/4K
	La solución debe encontrarse en el cuadrante de Líderes de Gartner para Data Center Networking. Certificaciones: FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2
CERTIFICACIONES	
CERTIFICACIÓN DISTRIBUIDOR AUTORIZADO: El proponente debe adjuntar carta del fabricante de los bienes y/o equipos, es distribuidor autorizado en Colombia. Donde se acredite estar en capacidad técnica de configurar, mantener y dar soporte técnico de los equipos.	

Especificaciones técnicas del bien o servicio GESTOR DE BACKUP

ITEM 3	**VEEAM BACKUP**
CARACTERÍSTICAS	**REQUERIMIENTOS MÍNIMOS**
Fabricante y modelo	VEEAM BACKUP
CARACTERÍTICAS ACTUALES	
TYPE	El licenciamiento del software de Backup requerido para la actualización se deberásuministrar en modalidad de soporte y actualización de la herramienta por el período de 1 año. El servicio de veam backup deberá tener 30 licencias de Veeam Data Platform Premium para mecanismo de recuperación ante desastres La instalación e implementación de la herramienta debe ser realizada por parte del contratista con el personal idóneo capacitado por el fabricante.
CARACTERÍTICAS QUE DEBE CONTENER LA SOLUCION DE VEEAM BACKUP	
	• Servidor Veeam Recovery Orchestrator dedicado en Windows Server 2019 o superior. • Integración completa con Veeam Backup Server y Veeam ONE para inventario automático de backups, réplicas y planes de DR. • Soporte de DataLabs (mínimo 2) para pruebas aisladas, con capacidad para orquestar recuperación desde backups de Nutanix AHV y repositorios ExaGrid. • YARA Scan habilitado en: SureBackup, Secure Restore, Content Scan y planes de VRO. • Key Management System (KMS) Integration para gestión centralizada de claves criptográficas.

	• Four Eyes Authorization para operaciones destructivas (eliminación de backups/repositorios). • Malware Detection con Threat Hunter, IoC Scanner y Coveware Recon Scanner integrados en flujos de DR.

Respaldo en nube y restauración con capacidad de 150 TB

El servicio de respaldo en nube 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 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

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.
• Bases de datos en producción con motores SQL Server y PostgreSQL.
• Aplicaciones críticas para la gestión de procesos electorales y administrativos

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.
- 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.

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 24 horas para garantizar la integridad de la información.

Requisitos de Software y Seguridad

- 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

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

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.

Alcance del Servicio

El alcance del servicio estará enmarcado en la siguiente tabla que describe los aplicativos misionales de la entidad

Item	Aplicación	Descripción
1	Cuentas Claras 2011-2019	Aplicación de control de ingresos y gastos de las diferentes campañas políticas entre los años 2011 a 2019 un a aplicación por cada año
2	Cuentas claras 2023	Aplicación de control de ingresos y gastos de las diferentes campañas políticas entre los años 2022 a 2025
3	Cuentas claras 2026	Aplicación de control de ingresos y gastos de las diferentes campañas políticas año 2026
4	Portal Web	Portal web institucional
5	Aplicación software misionales	Aplicación para manejo de control electoral está constituido por 6 módulos diferentes (Distribución de espacios publicitarios, estatuto de oposición, cabildos, delegados escrutinios, veedurías ciudadanas, firmas encuestadoras)
6	RUPYM	Aplicación para el control de integrantes y militantes de los partidos políticos
7	Relatoría	Repositorio de autos y resoluciones
8	Sistema EPX	Sistema de gestión documental
9	Sistema ERP	Gestion de nómina inventarios y personal
10	Trashumancia	Aplicación control de trashumancia electoral
11	Hopex	Arquitectura empresarial
12	Ankara	Gestion de proyectos

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

Controles de Seguridad en la Infraestructura

- Protección de la infraestructura mediante firewalls aplicaciones Web (WAF) servicio en nube.
- Prueba de Ethical Hacking modalidad caja negra (una durante la ejecución del contrato), con análisis de penetración sobre los dominios establecidos por la supervisión del contrato (máximo 5 dominios) con el fin de establecer una línea base en temas de ciberseguridad.
- 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.

Monitoreo y Respuesta ante Incidentes

- Servicio de monitoreo continuo de 7 días a la semana por 24 horas (7X 24) 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.

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.

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.

Servicio de Firewall para Aplicaciones Web

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

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
  - 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 solución 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:
    - 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:
    - Visibilidad de aplicaciones Cloud usadas por el usuario.
    - Visibilidad de los sitios web más consultados por los usuarios.
- Visibilidad de las amenazas que han ocurrido en la red.
- Renovación y Soporte:
    - Renovación del soporte de firewall perimetral y Solución 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.

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.

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
  - Soportar al menos 8.8 Mpps
  - Fuentes simultáneas mínimo 1 millón
  - Soportar hasta 2 M queries DNS por segundo.
  - 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 automáticamente 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.

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.

Entregables y Reportes

El contratista deberá entregar los siguientes reportes y documentación:

Reportes de Seguridad

1. Informe de Monitoreo de Seguridad (mensual):

a. Eventos críticos detectados.
b. Análisis de incidentes de seguridad.
c. Medidas correctivas implementadas.

2. Reporte de Evaluación de Seguridad Perimetral (trimestral):
   a. Estado de la infraestructura de seguridad del CNE.
   b. Análisis de configuraciones y cumplimiento de mejores prácticas.
   c. Recomendaciones de mejora.
3. Informe de Pruebas de Ethical Hacking:
   a. Metodología aplicada y alcance de las pruebas.
   b. Vulnerabilidades detectadas y nivel de criticidad.
   c. Plan de remediación y mitigación.

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.

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 ANÁLISIS DE DISPONIBILIDAD, SEGURIDAD Y VULNERABILIDADES

Descripción General

El servicio de análisis de seguridad y 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 administrar la plataforma de seguridad y análisis de vulnerabilidades del CNE, asegurando visibilidad y control sobre los sistemas monitoreados. El servicio deberá operar bajo un esquema 7x24 y estar alineada con las mejores prácticas de seguridad, cumplimiento normativo y gestión de riesgos.

Monitoreo de Desempeño, Seguridad y Disponibilidad

El contratista deberá cumplir con los siguientes requisitos:

- Análisis en tiempo real del estado y disponibilidad de los servidores.
- Análisis y monitoreo de eventos de seguridad sobre la plataforma SIEM.
- SERVIDORES QUE SE ANALIZAN ACTUALMENTE:
  - **Servidores Windows:** 15 Servidores físicos e instancias de máquina virtual.
  - **Servidores Linux:** 10 Servidores físicos e instancias de máquina virtual.
  - **Hipervisores:** 6 Nodos de Administración NX
- DISPOSITIVOS DE RED:
  - **Firewalls:** 3 Firewalls FortiGate
  - **Switch Core:** 4 Switch Core
  - **Switches de Acceso:** 51 Switches de Acceso
  - **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.
- Monitoreo de alertas automáticas ante fallos o anomalías en el desempeño de los servidores.
- Monitoreo del registro histórico de métricas para análisis de tendencias y optimización de infraestructura.

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.

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.
  - Confirmación de correcta recepción de datos y generación de alertas.

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 preconfiguradas 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.
  - 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.

Servicio de Análisis de Vulnerabilidades

El contratista deberá realizar las tareas necesarias tendientes a establecer el estado actual de vulnerabilidad de la infraestructura tecnológica del CNE, este servicio debe contemplar el análisis de servidores virtuales, base de datos, portales web, se debe dimensionar el servicio para un máximo de 50 activos, los cuales serán definidos por la supervisión del contrato.

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).

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.

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.

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.

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 MISION CRITICA.

Replicación de Infraestructura Crítica

Se requiere replicar un total de 32 máquinas virtuales, que están contenidas en los servidores de hiperconvergencia actuales alojados en el Datacenter principal, la tabla siguiente contiene la línea base de máquinas a replicar, sin embargo esta puede ser modificada de acuerdo con las necesidades del CNE, sin superar un máximo de 50 máquinas virtuales

Ítem	Nombre	Rol	Estado	Condición	Espacio Aprovisionado	Espacio utilizado	Memoria de Host
1	ServHopex	Servidor aplicación Hopex	Encendido	Normal	365,08 GB	145,59 GB	16,1 GB
2	VM004-ERP-App	Servidor aplicación ERP	Encendido	Normal	255,28 GB	142,52 GB	16,09 GB
3	VM004-ERP-App-QA1	Servidor aplicación ERP	Encendido	Normal	147 GB	108,6 GB	16,06 GB
4	VM005-FileServer	Servidor de archivos	Encendido	Normal	1,2 TB	825,58 GB	2,04 GB
5	VM006-GLPI	Servidor aplicación GLPI	Encendido	Normal	120 GB	43,6 GB	7,97 GB
6	VM007-CuentasClaras 2011	Servidor cuentas claras antiguo	Encendido	Normal	724,24 GB	358,92 GB	16,07 GB
7	VM007-Kali	Servidor Seguridad Kali	Encendido	Normal	200,01 GB	113,15 GB	8,06 GB
8	VM008-PortalCapacitaciones	Portal capacitaciones QA	Encendido	Normal	239,41 GB	57,07 GB	8,05 GB
9	VM008-PortalesWeb	Portales web CNE	Encendido	Normal	530,23 GB	247,6 GB	24,12 GB
10	VM009-MySQL	Base de datos Mysql	Encendido	Normal	105 GB	36,02 GB	8,06 GB
11	VM011-ERP-BaseDatos	Base de datos ERP	Encendido	Normal	1,08 TB	551,57 GB	16,09 GB
12	VM012-cabildos	Aplicación cabildos	Encendido	Normal	532,34 GB	36,16 GB	8,06 GB
13	VM013-Mail	Mail proxy	Encendido	Normal	550,09 GB	34,11 GB	5,79 GB
14	VM014-Postgresql	Base de datos PostgreSQL	Encendido	Normal	600,09 GB	389,67 GB	16,1 GB
15	VM015-EPX-app	Servidor EPX	Encendido	Normal	1,22 TB	963,71 GB	16,09 GB
16	VM016-Encuestas ciudadanas	Servidor Encuestas ciudadanas	Encendido	Normal	280,86 GB	38,05 GB	8,06 GB
17	VM017-EspaciosPublicitarios	Servidor aplicación Espacios publicitarios	Encendido	Normal	255,07 GB	22,03 GB	8,06 GB

18	VM018-Intranet	Servidor Intranet	Apagado	Normal	513,55 GB	25,69 GB	0 B
19	VM019-Moodle-dlm	Servidor Moodle LMS	Encendido	Normal	505 GB	24,09 GB	7,05 GB
20	VM020-SQL-EPX	Base de datos EPX	Encendido	Normal	652,49 GB	360,86 GB	14,77 GB
21	VM021-Relatorias	Aplicación Relatorías	Encendido	Normal	510,09 GB	243,49 GB	8,06 GB
22	VM022-RUPYM	Aplicación Rupym	Encendido	Normal	1,8 TB	842,5 GB	16,09 GB
23	VM023-delegados	Aplicación delegados	Encendido	Advertencia	510 GB	19,23 GB	8,06 GB
24	VM024-Estatuto	Aplicación estatuto oposición	Encendido	Normal	510 GB	22,83 GB	8,07 GB
25	VM025-Trashumancia-Laravel	Aplicación Trashumancia Framework Laravel	Encendido	Normal	563,15 GB	61,25 GB	8,06 GB
26	VM026-Tribunales	Aplicación Tribunales	Encendido	Normal	510 GB	19,15 GB	8,06 GB
27	VM027-Veedurias	Aplicación Veedurias	Encendido	Normal	510 GB	18,93 GB	8,06 GB
28	VM028-SQL-PRD-hopex	Aplicación Hopex	Encendido	Normal	200 GB	64,32 GB	8,07 GB
29	VM028-URIEL	Servidor Aplicación Uriel	Encendido	Normal	510 GB	18,8 GB	8,06 GB
30	VM030-Escrutinio-Mesa	Servidor Aplicación Escrutinio	Encendido	Normal	2,15 TB	754,27 GB	9,78 GB
31	VM031-EscrutiniomesaBaseDatos	Servidor Aplicación Escrutinio	Encendido	Normal	420 GB	225,92 GB	3,51 GB
32	VM032-Centralizador	Servidor aplicación centralizador	Encendido	Normal	260,09 GB	17,14 GB	8,06 GB

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 en Datacenter alterno que permita la operación ininterrumpida de los sistemas críticos.

El proveedor deberá garantizar que toda la infraestructura esté alojada en un Datacenter Principal con certificación mínimo Tier IV Facility UPTIME Institute, Rated 4 Facilities TIA 942B, PCI DSS, ISO 27001, ISO 9001, el Datacenter deberá estar ubicado en Colombia, asegurando latencia mínima y mayor disponibilidad del servicio. Tambien deberá garantizar que el Datacenter alterno cumpla mínimo con las siguientes certificaciones. Tier III, del Uptime Institute y ubicado en Colombia.

Requisitos Técnicos

- Replicación en Tiempo Real: Sincronización con la infraestructura de respaldo en las instalaciones del CNE en modalidad Activo-Pasivo.
- 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.

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.
- Sistemas de gestión documental y ERP.
- 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

Servicio de Colocation

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

Equipos que colocar en el Datacenter Principal

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
Hiperconvergencia Nutanix	6 nodos
Sistema de respaldo EXAGRID	3

Equipos que colocar en el Datacenter Alterno

Equipo	Cantidad
Hiperconvergencia Nutanix NX	3 nodos
Switch Core Fortinet	1
Servidor Lenovo	1

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.

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.

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)
  - Balanceadores (administrador de un balanceador)
  - 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%.

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 calle 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 las máquinas virtuales en ambiente productivo.
- **Canales de datos (MPLS):**
  - Un canal de 200M entre San Martin y la Registraduría.
  - 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 las máquinas virtuales en ambiente productivo.

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.

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	4
Técnico soporte en sitio nivel 1	1
Líder de servicios de infraestructura	1
Especialista en redes y seguridad	1
Desarrollador PHP, Laravel	1
Líder de mesa de servicios	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 funciónales, indicando el estado de la solicitud, el tiempo de respuesta y la solución implementada según la siguiente tabla de tiempos y prioridad.

Prioridad	Tiempo de atención	Tiempo de solución	Tiempo total
Urgente	1 hora	2 horas	3 horas
Alta	1 hora	4 horas	5 horas
Media	4 horas	12 horas	16 horas
Baja	8 horas	24 horas	32 horas

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. Realizar por parte del coordinador de mesa de ayuda o el personal que ejerza el rol de call center la priorización de solicitudes de acuerdo con su impacto y urgencia basado en los siguientes criterios:
    - Crítico: "caída total del servicio" o "usuario VIP inoperante".
    - Alta: Problemas que afectan la productividad total de la entidad, pero tienen un "workaround" temporal.
    - Media: configuraciones, software lento, problemas de acceso a plataformas para usuarios únicos.
    - Baja: Peticiones de información, cambios de instalaciones no esenciales, instalación de software adicional.
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.

Reportes:

Los reportes a la supervisión serán entregados una vez al mes y se deben incluir como mínimo:

- Cantidad de incidentes registrados y repetidos
- Tiempo de resolución de incidente
- Cantidad de incidentes por problema
- Tiempo hasta la identificación del problema
- Cuantos tickets de cada tipo de servicio hubo
- Estadísticas de la cantidad total de tickets del mes/periodo, cuales están resueltos, cuantos pendientes y el estatus de cada uno.
- Realizar informes de la operación.
- 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.
- Métricas de cumplimiento y registro de las diferentes actividades que se realicen durante la ejecución del convenio.

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 de atención	Tiempo de solución	Tiempo total
Urgente	1 hora	2 horas	3 horas
Alta	1 hora	4 horas	5 horas
Media	4 horas	12 horas	16 horas

Baja	8 horas	24 horas	32 horas

6. SOLUCIONES DE CIBERSEGURIDAD

Control De Acceso A La Red (NAC)

El Control de Acceso a la Red (NAC – Network Access Control) es una solución de seguridad diseñada para regular, supervisar y controlar quién y qué dispositivos pueden acceder a la red, así como en qué condiciones y con qué nivel de acceso. En entornos empresariales modernos, donde conviven usuarios, dispositivos corporativos, equipos personales (BYOD), IoT y sistemas de terceros, NAC se convierte en un componente esencial para reducir riesgos y fortalecer la postura de seguridad.

Una solución NAC permite identificar y perfilar dispositivos y usuarios en tiempo real, validando su identidad, tipo, estado de cumplimiento (postura de seguridad) y ubicación. Con base en esta información, el sistema aplica políticas dinámicas de acceso, permitiendo, restringiendo o segmentando el acceso a la red según criterios como rol del usuario, tipo de dispositivo, nivel de seguridad o contexto de conexión.

Además, NAC facilita la segmentación de la red mediante VLANs dinámicas, roles, políticas de firewall o integración con arquitecturas Zero Trust, minimizando la superficie de ataque y limitando el movimiento lateral en caso de una amenaza. También ofrece capacidades de detección y respuesta, como la cuarentena automática de dispositivos no conformes o comprometidos.

Desde el punto de vista de cumplimiento y gobierno, NAC proporciona visibilidad centralizada, registros detallados, alertas y reportes que apoyan auditorías y el cumplimiento de normativas como ISO 27001, GDPR, PCI-DSS y otras regulaciones de seguridad de la información.

En conjunto, el Control de Acceso a la Red actúa como la primera línea de defensa de la infraestructura, asegurando que solo usuarios y dispositivos autorizados, confiables y en cumplimiento puedan interactuar con los recursos críticos de la organización, alineándose con las mejores prácticas de seguridad modernas y estrategias de defensa en profundidad.

Se requiere una solución de NAC que conste de un appliance virtual con licenciamiento para controlar mínimo 1500 dispositivos.

6.1.1 Los recursos de cómputo para el appliance virtual deberán ser suministrados por el oferente.

- Debe estar en capacidad de gestionar al menos 1500 dispositivos concurrentes
- El licenciamiento debe ser perpetuo para la entidad, No se admiten suscripciones
- La implementación debe hacerse en alta disponibilidad
- Se debe incluir el soporte de fábrica por 24 meses
- La solución debe estar en capacidad de instalarse en Azure, HyperV, AWS, Vmware KVM

6.1.2 La solución NAC debe incluir los siguientes bloques funcionales.

- Visibilidad de red y perfilado de dispositivos conectados.
- Automatización del proceso de provisión de red en función del tipo de dispositivo que se esté conectando
- OnBoarding de nuevos dispositivos sencillo, versátil y potente.
- Endpoint Compliance: Permitiendo a la organización desplegar políticas asociadas a diferentes grupos de usuarios, verificando su cumplimiento y notificando las desviaciones, permitiendo configurar diferentes protocolos de remediación, desde acciones de aislamiento inmediatas a simples notificaciones, pasando por acciones diferidas.
- Identificación de amenazas, a través de la integración con otros elementos, y ejecución de acciones de remediación en función del evento.
- Gestión de invitados y usuarios externos: Fácil y rápida, sin necesidad de involucrar al personal de IT en el alta de nuevos usuarios externos por medio de patrocinadores o Sponsors.

6.1.3 La solución NAC debe ser agnóstica respecto a los fabricantes del equipamiento de acceso, tanto cableado como inalámbrico y por tanto válida en redes heterogéneas.

6.1.4 La solución NAC debe estar integrada con los dispositivos de red y seguridad existentes, y los que se incluyan en la nueva arquitectura.

6.1.5 Debe ser capaz de trabajar bien con agentes instalados en los endpoints, o bien sin agentes.

6.1.6 La solución NAC no puede ser dependiente de soluciones 802.1x y RADIUS, pero debe de ser compatible.

6.1.7 La solución debe tener incluidos los módulos de integración con terceros

6.1.8 La solución debe integrarse con el Firewalls, SIEM, Generador de Analítica, Sandbox, EDR y Honeypots

6.1.9 Perfilado de dispositivos

- La solución NAC debe tener capacidad para inventariar todos los dispositivos de la red, incluyendo equipamiento que no sea PC, como impresoras, Smartphones (Iphone, Android y Windows Phone), teléfonos IP, cámaras y otros dispositivos IoT que pudieran existir (biométricos…) y dispositivos OT.
- Debe poder utilizar al menos 20 métodos diferentes para identificar el tipo de dispositivo: DHCP fingerprint, NMAP scan, Vendor OUI, ubicación, puertos abiertos o información obtenida a través de agentes.
- Debe soportar el perfilado de dispositivos interactuando con el dispositivo mediante HTTP/HTTPS, SSH/Telnet o incluso interaccionando con el dispositivo a través de scripts diseñados a medida.
- Debe incluir un servicio dinámico de identificación de dispositivos IoT que comparta la información disponible sobre el dispositivo a perfilar con un servicio en Nube, que emplee técnicas de inteligencia que ayuden a la identificación del dispositivo.

- Debe soportar el perfilado de dispositivos Windows pertenecientes al domino mediante WMI o WINRM, utilizando canales seguros y validados mediante certificado.

6.1.10 Authentication y enforcement

- La solución debe permitir conectarse a la red corporativa solo a dispositivos autenticados/registrados, desplegando políticas de seguridad que bloqueen y aíslen dispositivos que no cumplan los criterios corporativos, enviándolos a un área de cuarentena sin necesidad de intervención por parte de los administradores de red.
- Debe ser capaz de autorizar los accesos mediante asignación dinámica de VLAN's y/o aplicando ACLs al puerto de acceso.
- Debe ser capaz de controlar escenarios en los que hay más de un equipo conectado a un puerto, asociando a cada equipo la VLAN adecuada, siempre que el equipo de acceso lo permita.
- Debe ser capaz de integrarse con los firewalls para asociar los dispositivos a reglas de seguridad concretas, en función del tipo de dispositivo.
- Debe permitir extender las políticas de seguridad al acceso VPN, ya sea SSL en modo túnel o IPSEC a través de una política de seguridad consistente.
- Debe soportar autenticación de máquina y usuarios, pudiendo autenticar un endpoint sin usar agentes.
- Debe de ser capaz de asociar al dispositivo atributos adicionales, como la ubicación, tipo de dispositivo, fabricante… además de los atributos del usuario conectado.
- Debe soportar opciones de autenticación flexibles, incluyendo 802.1X, autenticación WEB y autenticación MAC.
- Para despliegues 802.1X, debe poder actuar como Radius Proxy y como Radius local (TTLS/PAP, l TTLS/MSCHAPv2, PEAP/MSCHAPv2, TLS)
- Debe soportar integración LDAP y Microsoft Active Directory, sin necesitar ningún componente adicional, para desplegar políticas en función de su pertenencia a ciertos grupos.
- Debe soportar RADIUS Identity store.
- Debe soportar la detección y perfilamiento de sistemas operativos Chrome
- Integración de MDM incluida
- Debe soportar enforcement por medio de SSH/SNMP

6.1.11 Requisitos de Endpoint Compliance y Remediación

- La solución debe soportar inspección de los dispositivos tanto basada en agente (persistente y disoluble) como sin agente.
- La solución NAC debe ser capaz de realizar, al menos, las siguientes comprobaciones: service packs, nivel de parcheo, que haya instalado las actualizaciones críticas, Antivirus y AntiSpyware, servicios y procesos, certificados, existencia de archivos y cualquier entrada del registro de Windows.
- Debe contar con un Motor de correlación de eventos.

- La solución debe proporcionar un rol de cuarenta que se interactúe con los Sistemas de parcheo. De esta manera, los dispositivos corporativos que no cumplan los requisitos serán enviados a un portal cautivo de "auto remediación": Los equipos que no sean compliant debe de ser enviados a cuarentena dinámicamente, y o bien se le proporcionan instrucciones para la remediación o se ejecuta la remediación automática a través de sistemas como BigFix.

6.1.12 Gestión de invitados

- El Sistema de control de acceso debe proporcionar una plataforma flexible y eficiente de gestión de usuarios no corporativos, que permita manejar el acceso de aquellos usuarios con un acceso transitorio (típicamente invitados) o con un acceso más estable (contratistas externos).
- Debe permitir definir perfiles limitados que solo tengan acceso a la gestión de cuentas de invitados.
- Debe permitir altas masivas (p.e. para conferencias), autoregistros, registros esponsorizados o dados de alta por un administrador.
- Debe permitir autenticaciones por medio de redes Sociales.
- Debe permitir la opción de Aceptar invitados por medio de patrocinadores o Sponsors.
- Debe ser flexible y permitir la definición de diferentes perfiles, como invitados de corta /larga estancia, asistentes a conferencias o autorregistrados.

6.1.13 Gestión y Reporte

- El sistema de control de acceso almacena información crucial sobre la red, cuántos elementos hay conectados y sus características, cuántos cumplen la política de seguridad de la empresa … así como los eventos de seguridad que se puedan haber producido. También almacena información sobre eventos en la red (cambios en los puertos, conexiones…) que pueden ser de gran utilidad para realizar investigaciones después de que se produzca una investigación.
- La plataforma debe poder ser configurada usando REST API
- Debe ofrecer una consola de monitorización, reporting y troubleshooting que ayude a los administradores y operadores de helpdesk.
- La consola debe ser accesible a través de una GUI Web, sin necesidad de aplicaciones específicas.
- Debe permitir obtener, al menos, la siguiente información:
    - Eventos de conexión a lo largo del tiempo
    - Cambios en los puertos.
    - Eventos de seguridad detectados por la plataforma a lo largo del tiempo (por ejemplo, fingerprints que cambian, intentos de impersonación.
    - Eventos de seguridad recibidos de otras plataformas, y las acciones tomadas
    - Resultado de los escaneos de compliance (fallados, pasados)
    - Histórico de dispositivos conectados, última conexión.

6.1.14 Debe incluir plantillas de reportes, ejecutables bajo demanda o programados).
6.1.15 Debe permitir customizar los reportes.
6.1.16 Debe de incluir plantillas de despliegue de políticas.
6.1.17 Debe de permitir la opción de usar un Sistema de reporte y monitorización dedicado.

Solución DLP (Data Loss Prevention)

Una **Solución DLP (Prevención de Pérdida de Datos)** tiene como objetivo principal proteger la información sensible de la organización frente a fugas, accesos no autorizados, uso indebido o exfiltración, ya sea de forma intencional o accidental. En un entorno donde los datos constituyen uno de los activos más críticos del negocio, DLP se convierte en un pilar fundamental de la estrategia de ciberseguridad y cumplimiento normativo.

DLP permite **identificar, clasificar, monitorear y controlar** el flujo de información confidencial — como datos personales, información financiera, propiedad intelectual o datos regulados— a través de múltiples vectores: correo electrónico, navegación web, aplicaciones en la nube, endpoints, redes internas y dispositivos externos. De esta manera, se asegura que los datos solo sean utilizados y compartidos conforme a las políticas de seguridad definidas por la organización.

Además, DLP contribuye al **cumplimiento de normativas y estándares** como ISO 27001, GDPR, PCI-DSS, HIPAA u otras regulaciones locales, proporcionando visibilidad, trazabilidad y evidencia mediante alertas, reportes y registros centralizados. Esto no solo reduce el riesgo operativo y reputacional, sino que también fortalece los procesos de auditoría y gobierno de la información.

En conjunto con otras soluciones de seguridad (NGFW, análisis de logs, control de acceso y monitoreo continuo), DLP habilita un enfoque preventivo y proactivo, alineado con las mejores prácticas de **Zero Trust y defensa en profundidad**, garantizando la confidencialidad, integridad y disponibilidad de la información crítica del negocio.

La entidad se encuentra interesada en adquirir una solución DLP con las siguientes características

CARACTERISTICAS:

6.2.1 Se requiere una solución DLP que permita a la entidad a anticipar y prevenir el robo de datos.
6.2.2 La solución debe estar licenciada para 1200 Endpoints por un periodo de 24 meses
6.2.3 **Requerimientos técnicos**

- La solución debe prevenir la exfiltración y pérdida accidental de datos.
- La solución debe ser SaaS, en cloud, sin instalación de equipos ni colectores en tierra.
- La solución debe ser una sola licencia, que incluya todo lo solicitado sin modulos adicionales de componentes de seguridad no solicitados que puedan generar administraciones o coexistencia con diferentes configuraciones que no permitan centrarse en la función de DLP. No se permiten soluciones que deban incluir infraestructura en sitio como servidores o bases de datos.
- La solución debe inspección y clasificar comportamientos aun sin crear reglas mediante el uso de Machine Learning.

- La solución debe tener la posibilidad de incluir analistas dedicados a detectar fugas de información en caso de requerirse directamente de fábrica.
- La solución debe proporcionar visibilidad inmediata sobre el movimiento y la actividad de los datos.
- La solución debe proporcionar visibilidad inmediata sin políticas sobre el movimiento de datos y los procesos empresariales.
- La solución debe proporcionar un agente unificado que consolide todas las funcionalidades de monitoreo y bloqueo.
- La solución debe integrar aprendizaje automático desde el primer día para establecer una línea base de la actividad individual del usuario y utilizar algoritmos de análisis de comportamiento para detectar comportamientos típicos frente a comportamientos novedosos o anómalos.
- La solución debe proporcionar capacidades adicionales de análisis y analítica para ofrecer insights a nivel organizacional.
- La solución debe permitir a las organizaciones activar servicios y obtener visibilidad de riesgos de datos en minutos para proteger datos sensibles desde el primer día.
- La solución debe detectar y responder a la manipulación de datos y actividades anómalas utilizando IA y ML.
- La solución debe ser capaz de monitorear amenazas internas y empleados de alto riesgo.
- La solución debe aplicar políticas de riesgo interno con acciones de seguridad proactivas en tiempo real.
- La solución debe permitir activar servicios y obtener visibilidad de riesgos de datos en minutos para proteger datos sensibles desde el primer día.
- La solución debe mapear las actividades en un formato de MITRE.
- La solución debe identificar y mitigar amenazas internas a través de análisis avanzados de comportamiento de usuarios.
- La solución debe asegurar los datos en uso por aplicaciones SaaS y otras aplicaciones.
- La solución debe permitir políticas de protección de privacidad de datos como almacenamiento de datos y logs forenses en Datacenter de la compañía, colocar seudónimos a los nombres de las cuentas que se están investigando para que el analista no sepa a quien se hace la revisión e incluir la autorización de investigaciones fuera de la caja (out-of-the-box) por parte de analistas.
- La solución debe proporcionar visibilidad inmediata sin políticas sobre el movimiento de datos y los procesos empresariales.
- La solución debe proporcionar visibilidad integral de las interacciones de los usuarios con los datos en la nube y mantener la protección a medida que los datos se mueven fuera de la nube, asegurando la protección continua de la información sensible, independientemente de su ubicación o método de acceso.
- La solución debe monitorear y bloquear datos sensibles transferidos a través de navegadores web a dominios públicos externos (por ejemplo, Gmail, Yahoo, Hotmail).
- La solución debe fortalecer las defensas contra posibles brechas de datos derivadas de la exposición de datos empresariales a través del uso no autorizado de aplicaciones, incentivando a los empleados a usar herramientas autorizadas.

- La solución debe diferenciar entre datos sensibles transferidos a soluciones en la nube empresariales y soluciones en la nube personales (por ejemplo, Google Drive para Empresas vs. Google Drive Personal).
- La solución debe identificar el uso de Shadow AI y detener la carga de datos sensibles.
- La solución debe tener capacidades de inteligencia artificial o aprendizaje automático.
- La solución debe monitorear el uso de aplicaciones SaaS, incluyendo herramientas de Shadow AI como Gen-AI, e incorporar educación de usuarios basada en riesgos en el punto de acceso a datos sensibles.
- La solución debe cumplir con los requisitos de residencia de datos.
- La solución debe construir un inventario completo con puntuación de riesgo de las aplicaciones SaaS y herramientas GenAI utilizadas en toda la organización, con información sobre el ingreso, egreso y credenciales de datos.
- La plataforma debe monitorear la actividad en aplicaciones de inteligencia artificial (e.g., ChatGPT).
- La solución debe aplicar análisis de comportamiento de usuarios y entidades a gran escala.
- La solución debe incluir un asistente de IA que resuma y contextualice los datos asociados con actividades de alto riesgo para acelerar el análisis de incidentes.
- La solución debe analizar qué datos se están utilizando y cómo, permitiendo determinar la mejor respuesta.
- La solución debe proporcionar capacidades adicionales de análisis y analítica para ofrecer insights a nivel organizacional.
- La solución debe clasificar y rastrear datos en tiempo real para proporcionar visibilidad y protección de datos inmediata, sin necesidad de políticas predefinidas.
- La solución debe estar disponible en la nube para facilitar su implementación y escalabilidad, como un servicio SaaS
- La solución debe funcionar independientemente de la conexión de red y la ubicación.
- La solución debe utilizar tecnología de agente ligero compatible con sistemas operativos Windows, macOS y Linux para una implementación sin problemas y actualizaciones automáticas a escala empresarial. Las funciones deben ser similares en los tres sistemas operativos.
- Sistemas operativos soportados: Windows 10, 11, Windows server 2012 R2 y siguientes, MacOS Mojave 10.14 y siguientes, Red Hat Enterprise Linux 7 y siguientes, CentOS / y siguientes, Ubuntu 16.04 LTS y 17.10 y Debian 8 y siguientes
- La solución debe utilizar un agente escalable y ligero para recopilar y registrar datos.
- La solución debe permitir reducir los costos de ancho de banda, al no depender de un motor de escaneo de archivos basado en la nube.
- La solución debe proporcionar un agente unificado que consolide todas las funcionalidades de monitoreo y bloqueo.
- La solución debe utilizar agentes, extensiones de navegador y conectores en la nube para recopilar, enriquecer e indexar automáticamente la actividad a través de diferentes tipos de eventos (autenticación, web, email, aplicaciones, USB, creación de archivos, compartición y descarga de archivos).

- La solución debe integrar aprendizaje automático desde el primer día para establecer una línea base de la actividad individual del usuario y utilizar algoritmos de análisis de comportamiento para detectar comportamientos típicos frente a comportamientos novedosos o anómalos.
- La solución debe proporcionar visibilidad profunda en las actividades de los usuarios, el acceso a datos y los sistemas para prevenir la salida de datos sensibles.
- La solución debe incorporar funcionalidades que permitan educar a los usuarios sobre el manejo adecuado de datos.
- La solución debe proporcionar capacitación basada en riesgos para entrenar a los empleados a tomar las decisiones correctas basadas en la detección de comportamientos inaceptables, reforzar las políticas de seguridad corporativa y promover una buena higiene cibernética.
- La solución debe incluir notificaciones personalizadas y recordatorios para reforzar la conciencia sobre las políticas de seguridad y dirigir a los usuarios a alternativas aceptables cuando se detecten aplicaciones no autorizadas.
- La solución debe proporcionar notificaciones personalizadas y recordatorios para reforzar la conciencia sobre las políticas de seguridad y dirigir a los usuarios a alternativas aceptables cuando se detecten aplicaciones no autorizadas. Las notificaciones deben poder enviarse a través de diálogos en el Endpoint, correo electrónico, y mensajería (por ejemplo: Microsoft Teams, Slack, etc.
- La solución debe aplicar políticas adaptativas basadas en riesgos que consideren factores de riesgo y permitan decidir qué acciones tomar, como notificar a los usuarios a través de mensajería (por ejemplo: Microsoft Teams, Slack, etc., capturar forenses de archivos y pantallas, aislar o bloquear un endpoint, terminar un proceso o bloquear actividades de alto riesgo.
- La solución debe integrarse fácilmente con los sistemas y plataformas existentes en la organización.
- La solución debe proporcionar perfiles MDM, transmisión de eventos, webhooks y una API abierta para la integración con herramientas MDM, SIEM, SOAR, de automatización y de mesa de servicio existentes.
- La solución debe identificar y rastrear datos automáticamente según su origen, como sistemas de recursos humanos o repositorios de código fuente, sin necesidad de incluir reglas iniciales para la detección.
- La solución debe diferenciar entre datos sensibles transferidos a soluciones en la nube empresariales y soluciones en la nube personales (por ejemplo, Google Drive para Empresas vs. Google Drive Personal).
- La solución debe aplicar políticas de DLP y de riesgo interno basadas en el origen de los datos y si se utilizó una cuenta corporativa o no corporativa para la salida de datos.
- La solución debe incorporar conectores de Google Workspace y Microsoft Office 365.
- La solución debe monitorear y bloquear datos sensibles transferidos a través de navegadores web a dominios públicos externos (por ejemplo, Gmail, Yahoo, Hotmail).
- La solución debe mapear las actividades a una base de conocimientos de tácticas, técnicas y procedimientos de amenazas internas.

- La solución debe proporcionar visibilidad de datos, evaluación de riesgos y políticas de protección de datos listas para usar para proteger los activos de información críticos dentro y fuera de la red.
- La solución debe ayudar a cumplir con requisitos clave de cumplimiento, incluyendo PCI DSS, HIPAA, ISO 27001, NIST, PII, PHI, entre otros.
- La solución debe abordar los controles de cumplimiento normativo relacionados con la prevención de pérdida de datos con un esfuerzo mínimo utilizando políticas predefinidas de PII/PHI/PCI.
- La solución debe priorizar la privacidad bajo regulaciones como GDPR y CCPA.
- La solución debe utilizar técnicas de minimización de datos integradas, como la seudonimización y el almacenamiento forense localizado, para ayudar a los equipos de seguridad a detectar y mitigar amenazas mientras se protege la confidencialidad de los empleados.
- La solución debe minimizar los conjuntos de datos de investigación seudonimizados.
- La solución debe mapear las detecciones de actividades de alto riesgo a una base de conocimientos de tácticas, técnicas y procedimientos de amenazas internas y secuenciarlas automáticamente en incidentes con puntuación de riesgo para priorizar las investigaciones.
- La solución debe almacenar los registros forenses en centros de datos controlados por el cliente en la región.
- La solución debe incluir flujos de trabajo de autorización de investigación listos para usar para los analistas.
- La solución debe proporcionar un feed de actividad detallado y secuenciado en el tiempo que permita a los analistas ver la actividad de usuarios, datos y dispositivos antes, durante y después de un incidente.
- La solución debe permitir a los analistas de seguridad tomar acciones según la gravedad del riesgo, como mostrar un mensaje en pantalla al empleado, tomar una captura de pantalla, terminar un proceso, bloquear conexiones a un dispositivo o bloquear el teclado y el ratón de un dispositivo.
- La solución debe incluir gestión de casos integrada y reportes de riesgos que destaquen comportamientos descuidados, maliciosos y accidentales a lo largo del tiempo, permitiendo evaluar la efectividad de los controles de seguridad e identificar áreas de mejora.
- Los reportes deben poder exportarse fácilmente para compartir con la dirección.
- La solución debe proporcionar un dashboard para cumplimiento y auditoría.
- La solución debe soportar la generación de reportes personalizados basados en usuarios específicos.
- La solución debe soportar la generación de reportes personalizados basados en tipos específicos de datos.
- La solución debe soportar la generación de reportes personalizados basados en períodos específicos.
- Los reportes deben poder exportarse fácilmente para compartir con otras áreas de la entidad.
- La solución debe incluir reglas predefinidas para detectar prácticas de higiene cibernética deficientes, como la carga de archivos confidenciales a ubicaciones inesperadas, la conexión

a redes Wi-Fi no seguras, la inserción de dispositivos de hardware maliciosos o el uso de aplicaciones no autorizadas para almacenamiento en la nube o dispositivos USB.

- La solución debe monitorear y bloquear datos sensibles transferidos a dispositivos USB.
- La solución debe monitorear datos sensibles transferidos a través de aplicaciones de terceros (por ejemplo, Putty).
- La solución debe monitorear datos sensibles copiados mediante capturas de pantalla.
- La solución debe monitorear datos sensibles copiados a través de pulsaciones de teclas (por ejemplo, imprimir pantalla).
- La solución debe monitorear datos sensibles copiados a nivel de archivo/carpeta.
- La solución debe monitorear datos sensibles copiados a nivel de comando (por ejemplo, símbolo del sistema, terminal).
- La solución debe monitorear datos sensibles copiados/descargados a una máquina virtual sin agente de punto final.
- La solución debe soportar el rastreo de múltiples archivos compartidos por un usuario.
- La solución debe funcionar independientemente de la conexión de red y la ubicación.
- La solución debe soportar el monitoreo del movimiento de datos sensibles fuera de un conjunto definido de usuarios.
- La solución debe exportar un historial de todo el movimiento de datos dentro de la empresa, incluyendo datos provenientes de fuentes externas.
- La solución debe monitorear la descarga de datos sensibles por un usuario directamente desde una aplicación/servidor de aplicaciones.
- La solución debe proporcionar detalles de los datos sensibles descargados por un usuario durante un período especificado, incluyendo el número total de archivos, volumen de descarga, nombres de archivos y origen.
- La solución debe monitorear servicios y plataformas de correo electrónico (por ejemplo, MS Exchange, Office 365, Gmail, Outlook).
- La solución debe bloquear el montaje de unidades de almacenamiento removibles (por ejemplo, USB, HDD externo).
- La solución debe monitorear y bloquear datos sensibles impresos en impresoras físicas y/o PDF.
- La solución debe integrarse con otras herramientas de ciberseguridad (e.g., SIEM).
- La solución debe integrarse con la plataforma de logs y analítica de seguridad con la que cuenta la entidad
- La solución debe integrarse con Active Directory, Azure AD y soluciones LDAP de terceros.
- La solución debe soportar MFA (Autenticación Multifactor).
- La solución debe soportar SSO (Inicio de Sesión Único) con Active Directory, Entra ID, GCP, Amazon, AWS.

6.2.4 Servicios y soporte

- La solución debe incluir soporte directo con el fabricante en modalidad 7días a la semana por 24 horas (7X24).

- La solución debe incluir acceso a un equipo especializado directo de fábrica que brinde orientación remota sobre implementación, actualizaciones y operaciones de la solución DLP.
- La solución debe incluir un servicio de buenas prácticas llevado a cabo por el fabricante que incluya el análisis inicial, revisión de políticas a implementar, ajuste de la solución, recomendaciones y seguimiento durante el primer mes de implementación y seguimiento mensual y final de la solución implementada. Debe realizarse directamente por el fabricante de la solución, no puede ser realizado por el oferente.
- La solución requerida debe incluir la licencia para Control de dispositivos integrada, DLP en línea para web, correo, Cloud Drive y conectores de medio, Clasificación de datos en tiempo real, análisis de riesgo de aplicaciones SaaS y de Inteligencia Artificial generativa, Entrenamiento de riesgos a usuarios finales, Soporte de librerías de cumplimiento regulatorio, etiquetas de Microsoft MIP/AIP, archivos forenses, gestión de incidentes y secuencia de tiempo de actividad. El entrenamiento debe incluir permitir hacer una evaluación de la justificación de incumplimiento.
- La solución requerida debe incluir las licencias necesarias para monitoreo de actividades de usuario y equipo final, analítica de comportamiento con Machine learning, detección de manipulación de datos, aislamiento de usuarios finales y bloqueo en tiempo real, detección de incidentes con puntuación de riesgo, captura de pantalla para análisis forense, gestión de caso, librería de detección de riesgo asociado a mapas de Mitre ATT&ck, conectores de integración con Google workspace, Microsoft office 365 y controles de compartir archivos
- La solución debe ser ofertada por un periodo de 24 meses.
- El producto debe incluir servicio de mejores prácticas implementadas directamente por la fábrica o en su defecto por un partner de servicios autorizado por la fabrica

Sistema de control de acceso con reconocimiento facial.

Se requiere el suministro e implementación de un sistema de control de acceso con reconocimiento facial de 5 puntos, a instalarse en el edificio de Consejo Nacional Electoral CNE, cubriendo 5 entradas principales a las oficinas de la entidad. La solución deberá permitir el control de acceso de entrada y salida en los accesos indicados, y contemplando el alcance de control sobre 5 puertas para aproximadamente (2800) usuarios. Asimismo, la solución deberá incluir los módulos de control de acceso y control de visitantes, junto con un esquema de reportes configurable a las necesidades institucionales.

Ítem	Descripción	Cantidad
1	Descripción general de la solución Suministro, instalación, configuración y puesta en funcionamiento de un sistema integral de control de acceso con reconocimiento facial, a implementar en la sede de Consejo Nacional Electoral, orientado al control de ingreso y salida de personas en accesos definidos, garantizando seguridad, trazabilidad, control de visitantes y generación de reportes operativos.	1
2	**Alcance físico y cobertura** • Sede Consejo Nacional Electoral CNE • Cobertura total de 5 puertas, incluyendo: • Acceso entrada y salida. • Capacidad operativa para aproximadamente (2800) usuarios.	

3	**Componentes de la solución** La solución deberá incluir como mínimo: • 12 lectoras con reconocimiento facial. • Software de gestión de control de acceso, para administración centralizada. • 5 electroimanes con sus respectivos soportes • 5 botones de emergencia para apertura de puerta en caso de emergencia • Infraestructura lógica necesaria para la operación del sistema conforme a la arquitectura definida. • Y todos los elementos necesarios para el correcto funcionamiento del sistema • El contratista deberá hacer la instalación de todo el sistema y sus componentes en la sede de la entidad CNE.	
4	**Módulos funcionales incluidos** • Módulo de control de acceso, para gestión de ingreso y salida por reconocimiento facial. • Módulo de control de visitantes, permitiendo registro, seguimiento y control de accesos temporales.	

5	**Funcionalidades operativas y de gestión**
	
	• Gestión centralizada de usuarios y perfiles de acceso.
	• Configuración de reglas de acceso por puerta, piso y tipo de usuario.
	• Generación de reportes totalmente configurables, incluyendo:
	  ○ Control de visitantes.
	  ○ Control de tiempos de estadía de funcionarios.
	  ○ Horarios de ingreso y salida cuando el acceso esté controlado por reconocimiento facial.
	• Capacidad de adaptación a las necesidades operativas de la entidad	

6	**Soporte, mantenimiento y transferencia de conocimiento** • Un (1) mantenimiento preventivo cada 12 meses sobre los elementos que componen la solución. • Atención a fallas del sistema bajo esquema NBD (Next Business Day). • Transferencia de conocimiento al administrador designado por CNE, una vez instalado el sistema, para su correcta operación y gestión.	
7	**Consideraciones operativas** • La solución debe operar de forma integrada como un sistema único. • La implementación debe respetar la condición de puertas de emergencia, controlando la salida mediante botón donde aplique. • El sistema debe permitir escalabilidad operativa dentro de la infraestructura definida.	

ITEM	CONDICIONES TÉCNICAS MÍNIMAS		CUMPLE	NO CUMPLE
1.	**SUMINISTRO TERMINALES DE RECONOCIMIENTO FACIAL (CAPACIDAD 2800 ROSTROS)**			
1.1.	Cantidad	12		
1.2.	Marca	Especificar		
1.3.	Modelo	Especificar		
1.4.	Tipo	Terminal biométrico facial con base para montaje en pared o pedestal		
1.5.	Protocolo	IP		
1.6.	Conexiones de entrada/salida	LAN 10/100 Mbps, Wiegand x, RS-485 × 1, Tamper x 1, Señal contacto de Puerta x1, Señal Botón de salida x 1, control de cerrado de puerta X1		
1.7.	Pantalla LCD Incorporada	LCD táctil mínimo 4,5 pulgadas; de resolución mínima de 480 x 854.		
1.8.	Lectora de tarjetas	Incorporada, Mifare y/o M1		
1.9.	Capacidad Rostros	Mayor a 2.800		
1.10.	Capacidad Tarjetas	Mayor a 2.800		
1.11.	Capacidad eventos	Mayor a 120.000		
1.12.	Tiempo de reconocimiento facial	Menor a 0,3 segundos por persona con una tasa de precisión superior al 99%		
1.13.	Distancia de reconocimiento facial	Desde 0.4 metros a 1.3 metros o superior		
1.14.	Cámara óptica Incorporada	Cámara 2 MP		
1.15.	Verificación de rostro vivo	Soportado		
1.16.	Lectura de código QR	Soportado		
1.17.	Audio	Doble via		
1.18.	Alimentación	El oferente debe incluir la fuente de alimentación del terminal, la cual debe tener entrada 120-200 VAC, 60 Hz..		
1.19.	Temperatura de trabajo	-25 °C a 55 °C o superior.		
1.20.	Protección	IP65		
1.21.	Ficha técnica	Adjuntar en la respuesta a esta solicitud la ficha técnica del producto ofertado		

Protección de correo electrónico.

La protección de correo electrónico es un componente crítico de la estrategia de ciberseguridad de cualquier organización, ya que el correo sigue siendo el principal vector de ataque para amenazas como phishing, malware, ransomware, suplantación de identidad (spoofing) y fuga de información. Una solución moderna de seguridad de correo no solo debe filtrar mensajes maliciosos, sino también proteger a los usuarios, los datos y la continuidad del negocio.

Este tipo de solución proporciona protección avanzada antes, durante y después de la entrega del correo, combinando múltiples motores de análisis para detectar amenazas conocidas y desconocidas. Incluye capacidades como antispam de alta precisión, protección contra phishing y ataques de ingeniería social, análisis de adjuntos y enlaces en tiempo real, y detección de comportamientos anómalos en el contenido del mensaje.

Además, la protección de correo electrónico moderna integra seguridad colaborativa para el usuario final, permitiendo a los empleados reportar correos sospechosos, recibir alertas de riesgo y beneficiarse de procesos automáticos de remediación. Esto reduce significativamente el impacto del error humano y fortalece la conciencia de seguridad dentro de la organización.

Desde una perspectiva de protección de la información, estas soluciones incorporan funciones de prevención de pérdida de datos (DLP), cifrado, control de contenido y cumplimiento normativo, asegurando que la información sensible no sea enviada o compartida de forma indebida, ya sea de manera accidental o maliciosa.

Finalmente, la administración centralizada, la visibilidad completa del tráfico de correo, los reportes detallados y la integración con otros controles de seguridad permiten a las organizaciones responder rápidamente a incidentes, cumplir con regulaciones y mantener una postura de seguridad sólida frente a amenazas cada vez más sofisticadas.

En conjunto, la protección de correo electrónico orientada al entorno colaborativo y de productividad se convierte en un pilar fundamental para la seguridad del usuario, la protección de datos y la resiliencia operativa de la organización.

CARACTERISTICAS:

6.3.1 Escaneo de correo electrónico

- La solución debe analizar dinámicamente el 100% de los correos electrónicos
- La solución debe analizar todas las URL y archivos adjuntos de los correos electrónicos entrantes
- La solución debe escanear dinámicamente los correos electrónicos a una velocidad media de 15 segundos
- El administrador de la solución debe estar en capacidad de acceder automáticamente a los detalles del análisis para ver las razones exactas por las que se marca un correo electrónico como malicioso
- La solución debe proteger activamente contra el spam

- La solución debe identificar amenazas después de la entrega de correo. Debe estar en capacidad de notificar a los usuarios y recuperar correos electrónicos maliciosos de sus bandejas de entrada para ponerlos en cuarentena automáticamente

6.3.2 Identificación de amenazas

- La solución debe utilizar fuentes de inteligencia sobre amenazas para identificar amenazas conocidas
- La solución debe utilizar capacidades internas de búsqueda de amenazas asistidas por humanos
- La solución debe escanear los correos electrónicos de forma estática utilizando motores Antivirus
- La solución debe utilizar herramientas para identificar firmas muy complejas

6.3.3 Amenazas avanzadas

- La solución debe proteger contra los ataques de phishing a través del reconocimiento de imágenes, el análisis de texto y los evaluadores de reputación
- La solución debe proteger contra los ataques BEC cuando se realizan comprobaciones SPF, DKIM y DMARC
- La solución debe proteger contra los ataques de suplantación de identidad mediante el uso de técnicas para descubrir la suplantación de nombres de visualización y la suplantación de VIP
- La solución debe proteger contra ataques de día cero y día N al inspeccionar datos a nivel de CPU
- La solución debe detectar ATO mediante la observación de anomalías en el comportamiento del usuario

6.3.4 Manejo de URL

- La solución debe hacer clic y escanear activamente las direcciones URL para identificar enlaces maliciosos antes de que lleguen al buzón del usuario final

6.3.5 Sandbox

- La solución contar con la tecnología Sandbox para identificar archivos maliciosos
- La solución debe utilizar datos de nivel de CPU para inspeccionar el flujo de ejecución de archivos
- La solución debe mantener la integridad de los archivos durante los análisis, evitando alterar la estructura de los archivos
- La solución debe identificar vulnerabilidades de daño en la memoria
- La solución debe detectar errores lógicos y macros dentro de los documentos

6.3.6 Gestión de archivos

- La solución debe escanear cientos de tipos de archivos diferentes
- La solución debe descomprimir el contenido de forma recursiva, buscando enlaces y archivos incrustados para escanear
- La tecnología de la solución para escanear enlaces y archivos incrustados debe tener al menos 7 capas de profundidad

- La solución debe analizar contenido protegido con contraseña al entregarse el password
- La solución debe analizar archivos comprimidos/comprimidos

6.3.7 Situación del mercado

- La solución debe estar en la Guía de mercado de Gartner para la seguridad del correo electrónico
- La solución debe estar catalogada en los tres primeros lugares en la evaluación de SE Labs.

6.3.8 Protección de Navegadores

- La solución debe bloquear sitios de phishing de hora cero, sitios maliciosos, extensiones peligrosas en el browser en tiempo real.
- La solución debe instalar un agente liviano que no afecte el funcionamiento del navegador
- LA solución debe proveer una consola donde se indique un inventario de usuarios y browsers utilizados
- Debe permitir el modo de protección de riesgos (Silencioso, Precaución, Bloqueo como mínimo)
- Debe permitir personalizar las interfaces de usuario final para enviar precauciones, mensajes o bloqueos
- Debe permitir la integración con SAML
- Debe permitir asignar políticas con base en los permisos del usuario (atributos de sAML)
- Debe permitir el uso de Roles (RBAC)
- Debe permitir crear usuarios de administración y auditoria
- Debe estar en capacidad de realizar una correlación entre eventos del Browser y el correo.
- Debe soportar sistemas operativos Windows, MacOS, Chrome OS, Linux OS.
- Debe cumplir la integración con soluciones UEM para la implementación como Microsoft Intune, Jumpcloud, Jamf Pro, google Workspace.
- La solución debe usar modelos de Inteligencia Artificial para reconocimiento de imágenes y texto
- La solución debe permitir la instalación por medio de invitación de correo
- Debe ser compatible con cualquier infraestructura de red/proxy/VPN.
- La solución debe reforzar el acceso seguro a las aplicaciones web y SaaS mediante DLP para prevenir fuja de datos accidental o intencional interna o externa.
- La solución debe estar en capacidad de detener descargas de archivos y exploits de secuencias de comandos entre sitios (XSS)
- La solución debe estar en capacidad de administrar Google Chrome, Microsoft Edge, Firefox, Safari y cualquier otro browser con base en Chromium (ej Opera, brave, Arc, etc.).

6.3.9 Protección de herramientas de colaboración

- **Protección de Herramientas de colaboración**
    - La solución debe ser compatible con Slack, Microsoft 365 (Teams, One Drive, SharePoint) usando APIs.

- La solución debe detectar y bloquear archivos maliciosos, URLs, y ataques avanzados en las soluciones protegidas
- La solución debe proveer un servicio de Incident&Response (IR) para evaluar casos particulares o solicitados por el usuario final de 7x24
- Debe escanear el 100% de los datos
- La solución debe evaluar los correos y URLs que se envíen por las plataformas evaluadas
- El servicio debe tener un Objetivo de nivel de servicio de mínimo 99.98%
- Debe proveer servicios de Análisis de amenazas, Análisis dinámico y estático de archivos, protección de toma de cuenta (mínimo MS365)
- Debe proveer Gobernanza de los navegadores y DLP

- **Servicio alojado en la nube**
  - La solución debe ser nativa de la nube y está totalmente alojada en la nube
  - La solución debe actualizarse automáticamente
  - La solución debe satisfacer las necesidades de escalamiento de licenciamiento de un cliente sin afectar la experiencia del usuario ni requerir la compra de equipos adicionales
- **Instalación**
  - La solución debe permitir la implementación en modo de prevención de amenazas, evitando las amenazas antes de que lleguen a los usuarios finales
  - La solución debe permitir ser implementada en modo CCO/Journaling, así como en línea para una protección completa en M365 como mínimo
  - La solución debe permitir la implementación para los usuarios a través de una invitación por correo electrónico
  - La solución debe ser implementada automáticamente con la integración de Office 365 y Google Mail
- **integración**
  - La solución debe tener la posibilidad de conectarse a través de API a otras aplicaciones.
  - La solución debe integrarse con Office 365 a través de API sin necesidad de cambiar el registro MX.
  - La solución debe poderse ajustar a las políticas y SIEM existentes y no requiere cambios en la infraestructura e integración vía REST APIs
  - La solución debe estar en capacidad de exportar registros en tiempo real al SIEM
  - La solución debe estar en capacidad de integrarse con gestores de Identidades a través de SAML.
  - Los usuarios se deben asignan automáticamente permisos a roles y grupos en función de un esquema RBAC.
  - La solución debe estar en capacidad mediante licencias adicionales de proteger el uso del cliente del almacenamiento compartido, las herramientas de colaboración y el navegador.

- **Gestión de datos**
    - La solución debe cifrar los datos en reposo con AES-256 y en tránsito con TLS 1.2+
    - Las claves de cifrado deben estar protegidas con soluciones como AWS KMS
    - La solución debe cumplir con: SOC2, GDPR, HIPAA, ISO 27001
    - La solución debe estar alojada en servidores separados ubicados en Europa, EE. UU. y APAC para garantizar resiliencia del servicio
- **Gestión**
    - La solución debe proporcionar un panel de administración informativo que muestre datos de incidentes, informes y políticas
    - la solución debe tener la opción de incluir en las listas negras o blancas en función de la IP, las URL, los dominios, los remitentes, los tipos de archivos, etc.
    - La solución debe registrar las acciones del usuario, como los intentos de inicio de sesión, los cambios en el veredicto, la publicación de correos electrónicos y las solicitudes de investigación
    - El cliente debe estar en capacidad de personalizar los banners y las alertas de advertencia y traducirlos a otros idiomas como español, inglés y portugués
    - La solución debe tener una forma que el usuario reporte un presunto falso positivo o falso negativo para que la solución la revise y de su veredicto
    - La solución debe enviar informes y resúmenes de acciones a los usuarios

6.3.10 Servicio.

- **Respuesta a incidentes**
    - La solución debe contar con un equipo interno de Incident&Response (IR) para reforzar los servicios de detección y corrección de los correos
    - La solución debe proporcionar servicios complementarios de equipos Incident&Response (IR) como parte de la oferta sin cargo adicional directamente de Fabrica.
- **Soporte al cliente**
    - La solución debe ofrecer soporte al cliente y capacitación ilimitados según sea necesario sin cargo adicional durante la duración del contrato
    - El servicio de atención al cliente debe estar disponible las 24 horas del día, los 7 días de la semana por correo electrónico, chat y teléfono.
- **Duración**
    - El servicio debe entregarse por 24 meses para 1000 buzones de correo de la entidad

7. SALAS DE VIDEO CONFERENCIA

La entidad requiere la adecuación de tres (3) salas de videoconferencia, las cuales se encuentran en las instalaciones del CNE, estas deben cumplir con los siguientes requisitos técnicos por cada una de las salas:

Pantalla de Visualización

- Tamaño: LED de 75 Pulgadas
- Resolución: 4K UHD
- Brillo: Mínimo 350-400 nits.
- Uso: Grado comercial/profesional (operación 16/7 o 24/7), con encendido/apagado automático vía señal HDMI (CEC).
- Montaje: Soporte de pared reforzado con ajuste de inclinación.

Sistema Dual de Cámaras (Captura de Video)

El sistema deberá integrar dos unidades de captura con las siguientes especificaciones:

- Resolución: 4K a 30fps (mínimo).
- Tipo: Cámaras PTZ (Pan, Tilt, Zoom) con zoom óptico de al menos 12x.
- Inteligencia Artificial: Capacidad de Auto-Framing (encuadre automático) y Speaker Tracking (seguimiento del orador).
- Campo de Visión (FOV): Mínimo 90° para la cámara de plano general.
- Conectividad: USB 3.0 o salida IP (NDI) para integración con el procesador central.

Audio (Micrófonos de Mesa)

- Arquitectura: Mínimo 2 micrófonos de mesa por sala tipo "Beamforming" (con formación de haces para captar solo la voz humana).
- Cobertura: 360 grados con radio de captación de al menos 4.5 metros por micrófono.
- Procesamiento (DSP): Cancelación de eco acústico (AEC), supresión de ruido ambiental y control automático de ganancia.
- Funcionalidad: Botón de "Mute" físico con indicador LED de estado (Rojo/Verde) en cada unidad.

Procesamiento y Grabación (Hub Central)

Para garantizar la grabación y la gestión de las dos cámaras, se requiere un equipo dedicado (Mini PC):

- Procesador: Equivalente a Intel Core i7 de última generación (para manejo de video 4K sin latencia).
- Software Compatible: Certificado para Microsoft Teams, Zoom o Google Meet.
- Grabación:
    - Local: Capacidad de grabación en disco de estado sólido (SSD) interno.
    - Nube: Integración nativa con servicios de grabación en la nube de la plataforma de VC utilizada.
- Interfaz de Control: Tableta táctil (Console) de 10 pulgadas para iniciar reuniones, cambiar cámaras y activar la grabación con un solo toque.

Instalación y Puesta en Marcha

Para la implementación de las salas, se debe cumplir con los elementos de instalación:

- Cables: Todos los cables deben estar debidamente canalizados y etiquetados.
- Configuración de Escenas: El proveedor debe configurar al menos 3 "presets" de cámara (Mesa completa, Puesto de expositor, Tablero).
- Pruebas de Grabación: Se debe realizar una prueba de estrés grabando una sesión de 60 minutos para verificar la sincronía de audio y video.

8. 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 con el proveedor actual no superará los 30 días calendarios, garantizando la continuidad del servicio, sin generar interrupciones que afecten la operación de la entidad.

Para tal fin, se establecen las siguientes condiciones obligatorias: 7días a la semana por 24 horas (7X24).

Transición sin Costo para el CNE:

El proponente adjudicatario deberá asumir el costo, sin que ello represente erogación alguna para el CNE, dándole trámite a 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.

Plan de Transición Detallado:

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

- Un cronograma de actividades que deberá ser entregado a la entidad en un plazo no mayor a 2 días hábiles de la firma del Acta de inicio, relacionando las 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.

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 de 7 días a la semana por 24 horas (7X24) y respuesta a incidentes.
   - Implementación y gestión de firewalls perimetrales y de aplicaciones (WAF).
   - Análisis de vulnerabilidad y pruebas de penetración (Ethical Hacking).
   - Detección, prevención y mitigación de amenazas cibernéticas.
3. Servicio de Monitoreo de Seguridad y Análisis de Vulnerabilidad:
   - Supervisión de desempeño y disponibilidad de la infraestructura tecnológica.
   - Escaneo periódico de vulnerabilidad 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.

Mesa de Ayuda:

- Atención de incidentes, solicitudes y requerimientos operativos bajo un esquema de 7 días a la semana por 24 horas (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.

Condiciones sobre la Infraestructura Existente:

- Propiedad de los Elementos Actuales: Se deja constancia 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 se contará con los recursos tecnológicos 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.
- Acceso a la Información Histórica: El proponente adjudicatario 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.

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.

Supervisión y Seguimiento:

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

9. 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 requerido.

ANS (Acuerdo de Niveles de Servicio)			
Servicio	**Descripción**	**Factor de Medición**	**Penalidad, Compensación**
Respaldo y restauración de información.	Hace referencia a la cantidad de respaldos realizados en el periodo.	Numero de respaldos realizados ---------- x 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 ---------- x 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 ---------- x 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 ---------- x 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 ---------- x 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 rendimiento y de consumo de recursos por 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 ---------- x 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

ANS (Acuerdo de Niveles de Servicio)			
Servicio	**Descripción**	**Factor de Medición**	**Penalidad, Compensación**
Servicio de interconexión entre sedes.	Mide la disponibilidad de los canales de datos e internet	Número de Horas servicio disponible ---------- x 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 ---------- x 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 ---------- x 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, se debe establecer un indicador individual para cada nivel (critico,alto,medio,bajo)	Numero de tikets resueltos dentro de los tiempos ---------- x 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



LUIS ARNULFO MORALES

Jefe Oficina de Tecnologías de la información