ANEXO 1 ESPECIFICACIONES TÉCNICAS

OBJETO:

Adquisición de una plataforma de navegador corporativo seguro (Browser corporativo) para 2.500 usuarios por 12 meses que incluya instalación y soporte.

1. ALCANCE

El Fondo Nacional del Ahorro S.A. requiere la contratación de una solución de acceso seguro para usuarios, aplicaciones, servicios y datos, orientada a fortalecer el acceso remoto e híbrido mediante un espacio de trabajo seguro basado en navegador y acceso Zero Trust.

De acuerdo con esta necesidad, el FNA requiere:

- Suscripción de licenciamiento de una solución de espacio de trabajo seguro basada en navegador, que permita el acceso controlado a aplicaciones corporativas autorizadas para usuarios internos, terceros, contratistas, usuarios remotos y dispositivos no administrados o BYOD.
- Habilitación de controles de seguridad y protección de datos durante la sesión del navegador, incluyendo restricción o control de carga y descarga de archivos, copiado y pegado, impresión, captura de pantalla, uso de sitios o aplicaciones no autorizadas de acuerdo con las políticas de la Entidad.
- Implementación de capacidades de acceso Zero Trust para aplicaciones privadas, aplicando políticas basadas en identidad, grupos de usuario, aplicación, contexto de acceso y principio de mínimo privilegio, reduciendo la exposición de aplicaciones internas y la dependencia de accesos amplios tipo VPN tradicional.
- Implementación de protección DNS mediante servicio DNS seguro, con capacidad de aplicar políticas de filtrado, permitir o bloquear dominios por categorías o listas definidas, proteger la navegación frente a dominios maliciosos o de riesgo y generación de reportes.
- Implementación de monitoreo de correo corporativo en Microsoft 365/Office 365 orientado a brindar visibilidad, análisis, trazabilidad y generación de eventos sobre la actividad de correo.
- Integración de todos los nuevos componentes y servicios bajo una única consola SaaS de administración centralizada, basada en políticas y perfiles.

2. ESPECIFICACIONES TÉCNICAS

La solución propuesta deberá contemplar una arquitectura de acceso seguro y protección avanzada para usuarios, aplicaciones y datos, orientada a fortalecer el trabajo remoto, híbrido y el acceso de terceros mediante un navegador seguro basado con capacidades de Zero Trust, protección DNS y monitoreo de correo corporativo.

La solución propuesta deberá contar con una plataforma SaaS de administración centralizada en alta disponibilidad.

El contratista deberá suministrar licenciamiento por doce (12) meses para 2.500 usuarios.

Durante la ejecución del contrato, el contratista deberá asegurar el cumplimiento de los siguientes requerimientos técnicos mínimos:

Requerimientos Navegador empresarial seguro (Browser corporativo)

- Deberá proveer un navegador empresarial seguro y endurecido, basado en tecnología Chromium, que permita proteger el acceso a aplicaciones web, aplicaciones SaaS y recursos privados, manteniendo una experiencia de uso familiar para el usuario
- Deberá permitir acceso unificado a recursos corporativos autorizados, aplicando controles granulares de navegación y acceso web mediante políticas centralizadas.
- Deberá proteger a usuarios y datos durante la interacción con aplicaciones web, SaaS y recursos privados, aplicando controles de seguridad directamente en la sesión del navegador para reducir riesgos de fuga de información y accesos no autorizados.
- Deberá incluir capacidades de acceso Zero Trust para controlar y restringir el acceso a recursos privados, aplicaciones internas y entornos de nube privada, aplicando políticas basadas en identidad, grupos y postura del dispositivo.
- Deberá conectarse de forma segura a un gateway de acceso Zero Trust, habilitando acceso controlado a aplicaciones internas y recursos privados autorizados.
- La solución deberá suministrar un navegador empresarial seguro que cuente con actualizaciones, parches de seguridad y permita consultar la versión instalada.
- Las políticas de acceso del navegador empresarial seguro deberán permitir evaluar postura del dispositivo considerando, como mínimo, sistema operativo Windows o macOS y estado de cifrado de disco mediante BitLocker en Windows o FileVault en macOS, antes de permitir, advertir o bloquear el acceso

- Deberá permitir la instalación individual del navegador empresarial seguro en dispositivos Windows de 64 bits, soportando como mínimo Windows 10 y Windows 11, y en dispositivos macOS con procesadores Intel x86 y Apple Silicon ARM64, soportando como mínimo macOS Sonoma 14, macOS Sequoia 15 y macOS Tahoe 26.
- Deberá permitir el despliegue masivo del navegador empresarial seguro en dispositivos Windows mediante Microsoft Intune y dispositivos macOS mediante Jamf Pro.
- Deberá permitir identificar y controlar el uso de aplicaciones de inteligencia artificial generativa basadas en web, con el fin de reducir riesgos asociados al uso no autorizado o no aprobado por la Entidad.
- Deberá soportar acceso seguro a sesiones RDP y SSH hacia recursos privados, a través del navegador empresarial seguro integrado con el componente de acceso Zero Trust.
- Deberá permitir controlar acciones de datos dentro de la sesión del navegador, incluyendo carga y descarga de archivos, copiar, cortar, pegar, impresión, guardado de páginas, captura de pantalla y compartición de pantalla, según las políticas definidas.
- Deberá evaluar la postura del dispositivo considerando sistema operativo Windows/macOS y cifrado de disco mediante BitLocker o FileVault, permitiendo definir acciones de permitir, advertir o bloquear el acceso según las políticas configuradas.
- Deberá incluir inteligencia de amenazas para clasificación y reputación de dominios y URLs, así como controles de análisis y protección sobre archivos transferidos mediante cargas y descargas.
- Deberá proporcionar visibilidad, registros y reportes de eventos asociados a navegación, autenticación, usuarios, aplicaciones y transferencia de archivos desde una consola centralizada de administración.
- Deberá permitir identificar y controlar el uso de aplicaciones SaaS, con el fin de restringir aplicaciones no autorizadas o de riesgo conforme a las políticas de la Entidad.
- Deberá permitir aplicar controles de prevención de fuga de datos dentro de la sesión del navegador, incluyendo como mínimo copiar, pegar, capturas de pantalla, impresión, carga de archivos y descarga de archivos.
- Deberá habilitar protección y aplicación consistente de políticas para usuarios remotos e híbridos, manteniendo una experiencia de uso transparente para el usuario final.
- Deberá habilitar acceso seguro a aplicaciones y recursos corporativos para terceros, contratistas, visitantes y usuarios externos autorizados, incluso desde dispositivos no administrados, bajo políticas centralizadas.

- La plataforma deberá permitir consultar registros y eventos asociados a navegación, usuario, correo electrónico, sistema operativo, política aplicada, URL/dominio, aplicación y resultado del evento, incluyendo eventos permitidos, advertidos o bloqueados.
- Deberá permitir crear listas de sitios para agrupar direcciones IP, dominios o URLs, y utilizarlas como objetos dentro de políticas web.
- Deberá soportar integración con Directorio Activo on-premises o Microsoft Entra ID como fuente de sincronización de usuarios y grupos.
- Deberá soportar autenticación federada como único método de inicio de sesión, así como un esquema mixto que permita autenticación federada y credenciales propias de la plataforma.
- La solución deberá permitir forzar que el acceso a aplicaciones SaaS críticas se realice exclusivamente desde el navegador empresarial seguro, mediante integración con Microsoft Entra ID y políticas de acceso condicional que permitan bloquear el acceso desde navegadores no autorizados.

Requerimientos de protección Navegación Web (SWG)

- La solución deberá permitir controlar las actividades de navegación web de los usuarios mediante políticas centralizadas.
- La solución deberá incluir una política base predeterminada, utilizada por defecto cuando no existan políticas personalizadas aplicables.
- La solución deberá permitir modificar la política base para definir acciones predeterminadas acordes con los lineamientos de seguridad de la organización.
- La solución deberá permitir aplicar políticas de navegación web con base en usuarios, grupos de usuarios, sistema operativo, cifrado de disco, aplicaciones, listas de sitios y categorías web.
- La solución deberá permitir definir restricciones sobre descargas y cargas de archivos durante la navegación web.
- La solución deberá permitir establecer controles de intercambio de datos durante la navegación web, incluyendo acciones sobre portapapeles, impresión, guardado de páginas, captura de pantalla y compartición de pantalla.
- La solución deberá permitir crear y gestionar objetos de política, incluyendo como mínimo postura del dispositivo basada en sistema operativo y cifrado de disco, grupos de aplicaciones, listas de sitios y categorías web.
- La solución deberá permitir aplicar controles de acceso basados en la postura del dispositivo, de modo que las políticas del navegador empresarial seguro puedan restringir automáticamente el acceso considerando, como mínimo, el

sistema operativo, el estado de cifrado de disco y la detección de protección endpoint instalada antes de permitir, advertir o bloquear el acceso.

- La solución deberá permitir definir y aplicar políticas web en función de la postura del dispositivo, incluyendo como mínimo plataforma del sistema operativo Windows/macOS, estado de protección de endpoint y estado de cifrado completo de disco con BitLocker en Windows y FileVault en macOS.

Requerimientos de protección DNS

- La solución deberá ofrecer protección DNS como servicio de resolución DNS segura, con controles de políticas e informes integrados en la consola centralizada. El servicio deberá permitir agregar las ubicaciones que se desean proteger, especificando las direcciones IP públicas de las redes de la Entidad, y actualizar la configuración DNS de las redes o dispositivos compatibles para usar protección DNS.
- Este servicio deberá permitir la aplicación de políticas centralizadas de filtrado, bloqueo de dominios maliciosos o de riesgo, administración de listas permitidas o bloqueadas, clasificación por categorías y generación de registros para visibilidad e investigación.
- La solución deberá permitir mostrar páginas de bloqueo para dominios restringidos por política y suministrar el certificado requerido para su despliegue manual o mediante herramientas de administración de la Entidad, cuando aplique.
- El servicio de protección DNS deberá permitir aplicar políticas centralizadas, permitir o bloquear dominios individualmente o por categoría, definir listas de dominios, gestionar respuestas de bloqueo y generar registros e informes para visibilidad, auditoría e investigación.
- La protección DNS propuesta deberá permitir políticas de filtrado por categoría web, listas de dominios personalizadas y precedencia de listas permitidas o bloqueadas sobre categorías.
- Deberá redirigir consultas DNS hacia el servicio de protección DNS mediante DNS sobre HTTPS, para ayudar a proteger el tráfico DNS frente a amenazas, dominios maliciosos y uso indebido.

Requerimientos ZTNA integrado para aplicaciones privadas

- Deberá incluir capacidades de Zero Trust Network Access integradas con el navegador empresarial seguro, permitiendo controlar, condicionar y restringir el acceso de los usuarios a recursos privados conforme a políticas definidas, considerando como mínimo identidad del usuario, grupos, aplicación, recurso publicado, condiciones de acceso y postura del dispositivo cuando aplique.

- El servicio ZTNA deberá integrarse con servicios de identidad corporativa, incluyendo Directorio Activo on-premises y Microsoft Entra ID, para consumir usuarios y grupos requeridos en la asignación de políticas de acceso.
- El servicio ZTNA deberá integrarse con Microsoft Entra ID como proveedor de identidad para la autenticación de usuarios y la aplicación de políticas de acceso a recursos privados, permitiendo complementar el flujo de autenticación con los controles de seguridad disponibles en el proveedor de identidad.
- La solución ZTNA deberá proporcionar acceso seguro a aplicaciones internas y recursos en entornos privados mediante un gateway de acceso seguro, utilizando cifrado TLS.
- El servicio ZTNA deberá permitir publicar recursos para acceso a través del gateway ZTNA y deberá soportar acceso sin agente para aplicaciones web.
- La solución deberá permitir el acceso a recursos privados desde el navegador empresarial seguro, de forma que el usuario pueda conectarse de manera segura al gateway ZTNA y acceder de forma controlada a aplicaciones internas y recursos privados.
- La solución deberá soportar acceso sin agente a sesiones remotas RDP y SSH, ejecutadas desde el navegador empresarial seguro.
- La solución deberá permitir aplicar controles de acceso a aplicaciones utilizando identidad, grupos, aplicación, recurso publicado, condiciones de acceso y postura del dispositivo cuando aplique.
- La solución ZTNA deberá ser administrada desde la misma consola centralizada de administración de la solución, sin requerir consolas independientes para la operación del componente ZTNA.
- La solución ZTNA deberá permitir aprovisionar y gestionar gateways, configurar políticas granulares de acceso y asociar aplicaciones o recursos privados a grupos de usuarios autorizados, soportando acceso sin agente para aplicaciones web y recursos soportados mediante el navegador empresarial seguro.
- El servicio ZTNA deberá soportar dos modos de despliegue del gateway: gateway provisto en la nube y gateway alojado en las premisas de la Entidad.
- El servicio ZTNA en modalidad cloud gateway deberá permitir seleccionar un punto de presencia o región, con el fin de optimizar la latencia hacia los recursos privados publicados.
- El servicio ZTNA en modalidad cloud gateway deberá permitir continuidad del servicio mediante punto de presencia secundario y failover automático entre el punto primario y el secundario.
- La solución deberá permitir desplegar gateways ZTNA locales en formato appliance virtual sobre infraestructura de virtualización suministrada por la

Entidad, compatible como mínimo con VMware ESXi 6.5 o superior y Microsoft Hyper-V 2016 o superior.

- El servicio ZTNA deberá integrarse con servicios de identidad corporativa, incluyendo como mínimo con Microsoft Active Directory on-premises y Microsoft Entra ID, para consumir usuarios y grupos requeridos en la asignación de políticas de acceso.
- En caso de requerirse modalidad de acceso ZTNA con agente para aplicaciones no web o recursos privados que requieran conectividad desde el dispositivo del usuario, el agente ZTNA deberá estar soportado, como mínimo, en Windows 10 versión 1803 o superior y macOS Big Sur / macOS 11 o superior.
- La solución deberá permitir controles de acceso ZTNA basados en identidad, grupos, aplicación, recurso publicado, condiciones de acceso y postura del dispositivo cuando aplique según el modo de acceso configurado.
- El despliegue del gateway ZTNA local deberá soportar dos modos de conexión de red: una sola interfaz para tráfico entrante y saliente, y dos interfaces separadas para tráfico externo e interno.
- Cuando se habilite modalidad de acceso ZTNA con agente, la solución deberá permitir configurar parámetros operativos del túnel entre el agente y el gateway.
- La solución de acceso Zero Trust deberá permitir administrar dominios y certificados del servicio, incluyendo la generación de certificados mediante Let's Encrypt.
- La solución deberá permitir definir el acceso a aplicaciones privadas mediante gateway ZTNA y recursos publicados por FQDN o IP interna, de acuerdo con la topología definida por la Entidad.
- La solución de acceso Zero Trust deberá soportar el acceso a recursos que utilicen autenticación NTLM mediante el gateway. Asimismo, deberá permitir deshabilitar connection pooling cuando existan recursos sin agente que utilicen NTLM o métodos de autenticación similares, para asegurar compatibilidad operativa.

Requerimientos de Monitoreo de Correo

- La propuesta debe incluir capacidad de monitoreo de correo deberá soportar ingesta por journaling, recibiendo una copia de los correos según reglas definidas en el servicio de correo de la Entidad Microsoft 365.
- El módulo de monitoreo de correo deberá operar sin modificar el correo original y sin impedir su entrega al destinatario, realizando el análisis sobre una copia journal del mensaje.

- La solución deberá permitir generar registros de correo y mantener visibilidad sobre historial de mensajes, mensajes en cuarentena y reportes relacionados.
- La solución de monitoreo de correo deberá soportar recuperación manual post-entrega mediante integración API con Microsoft 365.
- La solución de monitoreo de correo deberá enviar datos relacionados a un Data Lake del proveedor, con el fin de aportar contexto adicional para actividades de detección, análisis, investigación y respuesta ante amenazas.
- La solución de monitoreo de correo deberá permitir configurar políticas de seguridad de correo y control de datos para generar veredictos de reporte, sin aplicar acciones de enforcement sobre los mensajes analizados.
- La solución de monitoreo de correo deberá permitir agregar buzones de monitoreo mediante sincronización automática desde Active Directory o Microsoft Entra ID, carga manual desde la interfaz de usuario e importación manual mediante archivo CSV.
- La solución de monitoreo de correo deberá permitir seleccionar el origen de journaling mediante opciones predefinidas para Microsoft 365 y Google Navegador Seguro/Gmail, así como permitir la definición de gateway personalizado mediante rangos IP o CIDR.

Requerimientos de Reportes

- La solución deberá contar con un módulo de reportes que permita seleccionar una plantilla de reporte, aplicar filtros, generar reportes, guardar plantillas y programar exportaciones.
- La solución deberá incluir plantillas de reporte, como mínimo, para uso web general, eventos de autenticación por usuario y transferencias de archivos realizadas desde el navegador empresarial seguro.
- La solución deberá permitir definir el rango de tiempo del reporte, incluyendo un rango personalizado con fechas y horas de inicio y fin.
- La solución deberá permitir exportar reportes en formato PDF, CSV o HTML.
- La solución deberá permitir definir el método de entrega del reporte, enviar el reporte mediante enlace a correo electrónico, exigir autenticación para abrir el enlace y permitir el envío del reporte a otros administradores de la consola.

3. Entregables (fases)

3.1 Planeación y Diseño:

Configuración Inicial piloto

- El contratista deberá ejecutar una prueba piloto controlada, sujeta a la validación funcional de los componentes incluidos en el alcance de la solución: Browser Corporativo, ZTNA, Protección DNS y monitoreo de correo.

  La configuración Inicial piloto deberá contemplar como mínimo:
  - Ambiente controlado para validar el acceso seguro desde el Browser Corporativo a aplicaciones web/SaaS autorizadas.
  - Validación básica de políticas aplicadas en la sesión del navegador, incluyendo controles de navegación y control de datos disponibles en la solución.
  - Validación básica de una política de Protección DNS y de eventos o registros generados en la consola centralizada.
  - Reporte de resultados:
    - Componentes configurados.
    - Políticas validadas.
    - Evidencia de acceso seguro desde el Browser Corporativo
    - Incidencias identificadas y su resolución, si aplica.

Plan de trabajo y cronograma

El Contratista deberá presentar, dentro de los quince (15) días hábiles siguientes a la firma del acta de inicio, en medio magnético, el plan de trabajo y cronograma para la implementación de la solución propuesta: navegador corporativo, ZTNA, protección DNS y monitoreo de correo.

El plan de trabajo deberá incluir, como mínimo:

- Gap inicial y análisis de brechas sobre los prerrequisitos requeridos para la implementación de Browser Corporativo, incluyendo identidad, usuarios, grupos, directorios, proveedor de identidad, DNS, certificados, conectividad, recursos a publicar, aplicaciones, mecanismos de despliegue del navegador protegido, protección DNS, monitoreo de correo y gateways ZTNA cuando aplique.
- Diseño de arquitectura de la solución, incluyendo diagramas de alto nivel, componentes licenciados, modelo de acceso con agente y/o sin agente cuando aplique, navegador corporativo, ZTNA, protección DNS, monitoreo de correo, usuarios, grupos, aplicaciones, recursos privados, gateways, políticas de acceso y consideraciones de conectividad requeridas para la operación de la solución.

- Suscripción de licenciamiento correspondiente a los componentes incluidos en la solución ofertada.
- Instalación, configuración, pruebas, puesta en marcha y estabilización de los componentes incluidos en el alcance contractual.
- Metodología de configuración, parametrización, administración y soporte de los componentes implementados, limitada a la solución objeto del proceso.
- Plan de transferencia de conocimiento funcional y técnico para mínimo dos (2) funcionarios definidos por la Entidad, orientado a la administración básica, operación, revisión de eventos, validación de políticas y escalamiento de la solución implementada.
- Plan de comunicaciones para la ejecución del proyecto, incluyendo responsables, canales de comunicación, reuniones de seguimiento y esquema de escalamiento.
- Plan de calidad y aceptación, teniendo en cuenta los hitos del proyecto, entregables definidos, criterios de validación funcional y ANS aplicables únicamente a los servicios y componentes incluidos en el alcance contratado.
- Actividades de revisión y estabilización operativa de la configuración implementada.
- Matriz de riesgos asociados a la ejecución del contrato.
- Seguimiento al cumplimiento de las obligaciones contractuales y especificaciones técnicas, conforme al alcance aprobado para la solución objeto del proceso.

El Contratista deberá considerar una metodología que le permita dimensionar, evaluar, instalar, implementar, configurar y transferir conocimiento (funcional y técnico), donde se tengan en cuenta todas las actividades y requerimientos necesarios para el cumplimiento del objeto del contrato, planteando de ser necesario etapas, recursos, entregables, así como las herramientas que considera necesarias emplear. Esta metodología deberá presentarse junto con el plan de trabajo.

Sin perjuicio de lo anterior, el Contratista deberá incluir y considerar todas las condiciones, recursos humanos, físicos, logísticos, etc., variables internas y externas para dar cumplimiento en calidad y oportunidad a la ejecución de las actividades y entregas, de conformidad con lo señalado en el capítulo Especificaciones Técnicas del presente documento.

Tiempo: Dentro del 30 días hábiles de ejecución del contrato.

El Contratista deberá atender las observaciones documentales realizadas por la Entidad y presentar los ajustes correspondientes dentro de un plazo máximo de cinco días hábiles, contado a partir de la recepción formal de dichas observaciones, siempre que los ajustes dependan directamente del Contratista.

Cuando la entrega o aprobación de los documentos dependa de información pendiente, definiciones técnicas, accesos, validaciones internas, aprobaciones de la Entidad o participación de terceros, el cronograma podrá ajustarse de común acuerdo entre las partes.

3.2 Implementación y configuración:

El Contratista deberá realizar la implementación y configuración de la solución conforme al diseño aprobado por la Entidad de:

- **Configuración de usuarios, directorios y autenticación:** Configuración de usuarios y grupos, ya sea mediante creación manual, sincronización desde directorio o integración con proveedor de identidad federado como Entra ID u Okta, según el modelo aprobado por la Entidad.
- **Configuración de política base:** Revisión, ajuste y validación de la política web base del navegador protegido, conforme a los perfiles de usuario, grupos, categorías web, listas de sitios y requerimientos definidos por la Entidad.
- **Despliegue del navegador protegido:** Despliegue del navegador protegido en los usuarios y equipos definidos por la Entidad, utilizando metodos tales como instalación manual, instalación silenciosa, Microsoft Intune para Windows/macOS o Jamf Pro para macOS, según aplique.
- **Configuración de protecciones adicionales:** Configuración y validación de las protecciones adicionales incluidas en la solución, contemplando protección DNS y ZTNA, de acuerdo con el alcance licenciado y el diseño aprobado.
- **Configuración de ZTNA:** Validación de los prerrequisitos técnicos y funcionales requeridos para la operación de ZTNA, incluyendo identidad, directorios, grupos de usuarios, dominio, certificados, DNS, conectividad y demás componentes necesarios conforme al diseño aprobado. La infraestructura requerida para alojar los gateways ZTNA en modalidad local será suministrada por la Entidad.
- **Despliegue de gateways ZTNA:** Aprovisionamiento y despliegue de los gateways ZTNA de acuerdo con el modelo aprobado por la Entidad, ya sea en modalidad cloud o en máquinas virtuales suministradas por la Entidad.
- **Configuración de recursos y políticas ZTNA:** Configuración de recursos, aplicaciones, grupos de aplicaciones, postura del dispositivo, categorías web, listas de sitios, usuarios, grupos y políticas de acceso Zero Trust conforme a las definiciones funcionales y técnicas de la Entidad.
- **Validación funcional:** Ejecución de pruebas de autenticación, validación de sesión, acceso por usuario, grupo y recurso, navegación protegida, resolución DNS, aplicación de políticas, operación de gateways, operación del agente y acceso sin agente cuando aplique.

- **Evidencias de implementación:** Entrega de evidencias generales de configuración, validación funcional y estado de los componentes implementados, conforme al alcance aprobado y a las actividades ejecutadas durante la fase de implementación.
  Plazo: Dentro del 60 días hábiles de ejecución del contrato.

3.3 Plan de transferencia de conocimiento y manuales

El Contratista seleccionado deberá presentar durante el segundo mes de ejecución del contrato, en medio magnético, el Plan de Transferencia de Conocimiento asociado a la solución implementada.

El plan deberá considerar como mínimo lo siguiente:

- Transferencia de conocimiento orientada a las tareas necesarias para el funcionamiento y el mantenimiento de los elementos que conforman la plataforma.
- Mecanismos y/o estrategias a emplear para la transferencia de conocimiento
- Lugar y plazo para la transferencia de conocimiento
- Información del personal que realizará la transferencia de conocimiento
- Temario que se llevara a cabo.
- El alcance de la transferencia deberá considerar temas de conocimiento técnico y funcional de la plataforma objeto del contrato.

La transferencia de conocimiento deberá realizarse dentro del plazo de ejecución del contrato, previa concertación de fechas con la supervisión contractual. Estará dirigida a mínimo dos (2) funcionarios de la Entidad, con una duración máxima de veinte (20) horas.

En las actividades de la transferencia de conocimiento se debe suministrar material didáctico e ilustrativo digital (PDF) que permita mejor comprensión de los temas en idioma español.

Así mismo, el Contratista deberá entregar mínimo los siguientes manuales, guías y memorias:

- Manual de configuración e instalación de los componentes de la plataforma
- Manual Funcional
- Manual Técnico
- Guía de Administración
- Memorias técnicas

Los manuales para entregar deberán ser actualizados a la última versión, según la dinámica requerida durante la ejecución del contrato.

3.4 Administración y soporte operativo de la solución

Este servicio de administración y soporte iniciará a partir de la puesta en operación de la solución de navegador corporativo empresarial y sus componentes y se mantendrá hasta la finalización del contrato.

El Contratista deberá prestar el servicio de administración (modalidad 5x8), operación, soporte técnico especializado y acompañamiento remoto únicamente cuando sea necesario y acordado con el contratista, sobre la solución implementada, garantizando su correcta operación conforme al alcance licenciado, el diseño aprobado, las políticas definidas por la Entidad y los componentes administrados desde la consola centralizada.

El servicio deberá orientarse a mantener la continuidad operativa de los componentes implementados en el presente proceso para el acceso seguro a aplicaciones SaaS autorizadas y aplicaciones privadas publicadas mediante ZTNA, incluyendo la administración de políticas basadas en identidad, contexto, postura, aplicación y condiciones de acceso**.**

Alcance del servicio ofrecido por el Contratista

El servicio deberá cubrir, como mínimo, las siguientes actividades:

- El Contratista deberá actuar como primer punto de contacto frente a la Entidad, realizar el diagnóstico inicial, recolectar evidencias, documentar los casos, ejecutar las acciones correctivas dentro de su alcance y escalar al fabricante cuando el caso corresponda a un evento asociado al producto licenciado.
- Monitoreo proactivo del estado de los componentes propuestos.
- Administración de políticas y configuración de los componentes de la solución ofrecida.
- Atender y resolver incidentes de la arquitectura.
- Soporte correctivo, preventivo y evolutivo.
- Acompañamiento y ejecución de cambios programados y/o de emergencia.
- Reportes periódicos de desempeño, capacidad y eventos relevantes.

Componentes a administrar

El Contratista deberá administrar y soportar los siguientes componentes implementados dentro del alcance de la solución:

- ✓ Consola centralizada de administración.

- ✓ Navegador corporativo empresarial.
- ✓ Políticas de navegación y controles aplicados durante la sesión.
- ✓ Zero Trust Network Access para aplicaciones privadas publicadas.
- ✓ Gateways ZTNA
- ✓ Agentes para los usuarios incluidos en el alcance.
- ✓ Recursos, aplicaciones, usuarios, grupos y políticas de acceso.
- ✓ Protección DNS para endpoints.
- ✓ Monitoreo de correo.

El Contratista deberá validar, antes del inicio de la prestación del servicio, la correcta configuración, operación y documentación de cada componente implementado, así como los accesos, dependencias técnicas, responsables, procedimientos de soporte y mecanismos de escalamiento requeridos para la administración de la solución.

Requerimientos del servicio Personal técnico del Contratista

- Personal especializado disponible remoto o en el sitio en la sede principal de la Entidad.
- Personal con acceso a herramientas de monitoreo y soporte del fabricante.

Horarios

- Soporte en horario 5X8 de lunes a viernes en el horario de 8 AM a 5 PM.
- Modalidad de soporte remoto con tiempos de respuesta definidos

Herramientas

- Uso de herramientas de monitoreo, diagnóstico y gestión compatibles con la solución.
- Acceso controlado y seguro a los componentes administrados.

Entregables del servicio

- Plan de administración y soporte, con procesos y responsables definidos.
- Reportes mensuales de desempeño y gestión.
- Actas de intervención y resolución por cada incidente atendido.

Esquema de atención diferenciado

El servicio de administración y soporte de la plataforma propuesta operará bajo el siguiente esquema diferenciado:

a. Monitoreo automatizado y alertas: 24 horas al día, 7 días a la semana (24×7). El Contratista deberá realizar seguimiento del estado operativo de la solución, revisión de eventos relevantes, alertas disponibles en la

consola centralizada y gestión de notificaciones configuradas para los responsables definidos por la Entidad.

b. Servicio de administración (remoto): de lunes a viernes en horario de 8:00 AM a 5:00 PM (5×8), excluyendo festivos nacionales.
c. Atención de incidentes críticos fuera del horario 5×8: el Contratista deberá garantizar un esquema de guardia (on-call) para la atención remota de incidentes de Severidad 1 (impacto severo en producción) fuera del horario, con un tiempo de respuesta no mayor a 2 horas desde la notificación.
d. Soporte técnico del fabricante (remoto): 24×7 para escalamientos de Nivel 3, conforme a la suscripción de soporte contratada.

El modelo de soporte operará bajo el siguiente esquema:

- Nivel 1 (FNA): recepción, registro, clasificación y escalamiento.
- Nivel 2 (Contratista): operación, configuración, análisis técnico y remediación.
- Nivel 3 (Fabricante): soporte especializado, correcciones de producto y escalamiento de ingeniería.

El contratista deberá presentar la matriz de escalamiento con tiempos de respuesta y solución dentro de los veinte (20) días hábiles siguientes al acta de inicio.

El modelo de atención del servicio se estructura de la siguiente manera:

i) Monitoreo y alertamiento automatizado: 24x7
ii) Soporte técnico remoto: 5x8
iii) Atención remota de incidentes críticos fuera de horario: esquema on-call
iv) Soporte del fabricante: 24x7

3.5 Requerimientos Mínimos Servicios Profesionales de Fabrica

El contratista deberá contemplar dentro de su propuesta incluir Servicios Profesionales del fabricante para apoyo en la implementación de la solución como mínimo con el siguiente alcance:

Servicios Profesionales de Fabrica para implementación de Navegador Seguro

- Configuración del navegador seguro dentro de la consola centralizada del fabricante para usuarios licenciados.

- Configurar controles de política del navegador empresarial para soportar acceso seguro a aplicaciones SaaS y recursos web internos, de acuerdo con los casos de uso definidos.
- Validar el comportamiento de acceso del navegador y la aplicación de políticas para los casos de uso iniciales acordados.

Servicios Profesionales de Fabrica para implementación de ZTNA

- Definir y configurar hasta tres (3) recursos protegidos y sus métodos de acceso, incluyendo el modelo de acceso correspondiente, ya sea con agente o sin agente, los requerimientos de nombres internos y externos, la asignación de grupos de usuarios y las políticas de control de acceso aplicables.
- Revisión de los prerrequisitos de despliegue de ZTNA, la selección del modo de implementación apropiado, ya sea gateway en premisas o gateway en la nube del fabricante, y la confirmación de los requerimientos asociados a plataforma de gateway, DNS, certificados y validación de dominio.
- Configurar y desplegar los componentes del gateway ZTNA, incluyendo, cuando aplique, el despliegue de la imagen del gateway, el registro del gateway, la asignación de certificados y la alineación de DNS público y privado.
- Validar el acceso a los recursos, la aplicación de políticas y la conectividad esperada del usuario, incluyendo la confirmación de comunicación del gateway y la alcanzabilidad de los recursos configurados.

Servicios Profesionales de Fabrica para implementación de Monitoreo de Correo

- Revisión del licenciamiento, alcance de buzones y prerrequisitos de despliegue del servicio de Monitoreo de Correo.
- Configurar el servicio inicial en la consola centralizada del fabricante, con base en el alcance acordado con la Entidad, y validar la visibilidad para los buzones seleccionados o los objetivos de monitoreo definidos.
- Revisar el flujo operativo para el monitoreo, revisión de alertas y administración diaria de la configuración implementada.

Servicios Profesionales de Fabrica para implementación de protección DNS

- Revisión del licenciamiento, ubicaciones protegidas o cobertura de endpoints, y prerrequisitos de despliegue de DNS Protection.
- Configuración de DNS Protection agregando las ubicaciones protegidas acordadas, actualizando la configuración DNS de red y alineando el tráfico DNS hacia el servicio de DNS Protection del fabricante.
- Configurar políticas iniciales de DNS Protection, incluyendo controles por categoría y configuración de dominios permitidos o bloqueados, de acuerdo con los requerimientos acordados con la Entidad.

4 Documentación

El Contratista y el personal que éste designe para realizar las diferentes labores objeto del contrato deberán garantizar la confidencialidad de la información del FNA a la cual tengan acceso directamente o por intermedio de terceros, así como la que genere, como producto de la ejecución de las actividades, y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros.

En ninguna circunstancia, dicha información y/o documentación podrá ser utilizada por el personal del Contratista para fines distintos al desarrollo de las actividades relacionadas con el cumplimiento del contrato.

4.1 Plan de trabajo y Cronograma

El Contratista deberá presentar a los cinco (5) días hábiles siguientes a la firma del acta de inicio, en medio magnético el plan de trabajo y cronograma, el cual deberá establecer entre otras, las actividades respecto de lo siguiente:

- Elaboración del Gap Inicial y análisis de brechas, con definición de acciones de mejora, donde se especifique el análisis realizado y evaluación del estado actual de los componentes.
- Diseño del diagrama de arquitectura que incluye las Características técnicas del nuevo modelo de arquitectura de control de acceso con todo el SW y servicios que hacen parte de este sistema.
- Suscripción de licenciamiento.
- Instalación, configuración, pruebas, puesta en marcha y estabilización de la solución o plataforma objeto del presente proceso.
- Metodología respecto a la configuración, parametrización, administración y soporte de la plataforma.
- Plan de Transferencia de conocimiento. El cual debe incluir una capacitación certificada por parte del fabricante en la administración de la plataforma objeto del presente proceso (2 personas mínimo).
- Plan de comunicaciones.
- Plan de calidad teniendo en cuenta la definición de ANS del servicio y del proyecto.
- Mantenimientos preventivos.
- Matriz de riesgos asociados a la ejecución del contrato.
- Seguimiento al cumplimiento de las obligaciones contractuales y especificaciones técnicas.

El Contratista deberá considerar una metodología que le permita dimensionar, evaluar, instalar, implementar, configurar y transferir conocimiento (funcional y técnico), donde se tengan en cuenta todas las actividades y requerimientos necesarios para el cumplimiento del objeto del contrato, planteando de ser necesario etapas, recursos, entregables, así

como las herramientas que considera necesarias emplear. Esta metodología deberá presentarse junto con el plan de trabajo.

Nota: La Entidad se reserva el derecho de ajustar aspectos de la metodología.

Sin perjuicio de lo anterior, el Contratista deberá incluir y considerar todas las condiciones, recursos humanos, físicos, logísticos, etc., variables internas y externas para dar cumplimiento en calidad y oportunidad a la ejecución de las actividades y entregas, de conformidad con lo señalado en el capítulo Especificaciones Técnicas del presente documento.

4.2 Plan de contingencia operativa

El Contratista seleccionado deberá presentar dentro del primer (1) mes, siguiente a la firma del acta de inicio, en medio magnético, el Plan de continuidad y contingencia de negocio, que permita evidenciar al FNA, las posibles anomalías que ponen en riesgo la correcta ejecución del contrato y que impidan el normal funcionamiento de la plataforma que se configure. Así mismo las medidas que se adoptarán para reanudar las operaciones ante las posibles fallas y/o perdida o degradación de la información objeto del presente proceso, que garanticen la continuidad del negocio.

El plan se limitará a los componentes efectivamente suministrados e implementados y a las actividades bajo responsabilidad del contratista. Incluirá los escenarios de falla aplicables, dependencias, contactos, escalamiento, comunicaciones, medidas de operación degradada y procedimientos de retorno a la normalidad. Los respaldos de configuración, mecanismos de restauración, *failover*, RTO y RPO se documentarán únicamente cuando sean técnicamente aplicables al componente correspondiente y estén respaldados por las capacidades y condiciones del fabricante.

Las pruebas de contingencia se definirán de común acuerdo durante la planeación y se ejecutarán sobre escenarios viables para la solución contratada. Este requisito no implica asumir la continuidad integral de los procesos de negocio del FNA, la recuperación de su información institucional ni la administración de infraestructura o servicios a cargo de terceros.

4.3 Hojas de Vida de los Componentes que conforman la Plataforma objeto del presente proceso

Las hojas de vida de los componentes que conformen la plataforma, deberán ser entregadas en medio magnético durante el primer mes posterior a la entrada en operación de la plataforma y deberán ser actualizadas, a los ocho (8) días hábiles contados a partir de la ejecución de cada mantenimiento preventivo y/o correctivo que se realice a los equipos,

componentes o software que hacen parte de la plataforma configurada, teniendo en cuenta los formatos y registros que FNA tiene destinado para este tipo de requerimientos

La hoja de vida de los equipos deberá informar entre otros los siguientes aspectos:

- Fecha de configuración y parametrización.
- Nombre o identificación de los equipos o componentes,
- Actividades realizadas en mantenimientos preventivos
- Actividades realizadas en mantenimientos correctivos
- Reemplazo de elementos y/o partes realizados en caso de que aplique según el tipo de servicio. Estado de funcionamiento
- Fecha próximo mantenimiento

Sin perjuicio de lo establecido en el presente capitulo, el Contratista deberá entregar todos aquellos documentos que el FNA requiera, relacionados con el desarrollo y ejecución del contrato.

4.4 Informes

El Contratista deberá entregar los siguientes informes en medio magnético en un formato de presentación estándar, redacción clara y buena ortografía.

4.4.1 Gap Inicial

Este informe deberá presentarse dentro de los quince (15) días hábiles siguientes al vencimiento del primer (1er) mes de ejecución del contrato, contados desde la firma del Acta de Inicio.

Nota: La razón para fijar el plazo al finalizar el mes 1 es garantizar que el Contratista cuente con tiempo suficiente para realizar el levantamiento técnico de los prerrequisitos, componentes, políticas y condiciones necesarias para la implementación de la solución Navegador Seguro antes de emitir el diagnóstico de brechas.

El informe deberá detallar, como mínimo, la siguiente información:

• Informe de GAP Analysis o diagnóstico inicial, en donde se plasme el análisis de brechas, definición de acciones de mejora y evaluación de los prerrequisitos requeridos para la implementación de la solución, incluyendo identidad, usuarios, grupos, directorios, proveedor de identidad, DNS, certificados, conectividad requerida para ZTNA, recursos a publicar, aplicaciones, mecanismos de despliegue del navegador corporativo, protección DNS, monitoreo de correo y componentes licenciados de la solución.

Así mismo, como actividad posterior a la entrega del Gap Inicial, se deberá:

• Actualizar el cronograma inicial una vez se cuente con el informe de GAP Analysis.

• Entregar el acta de recibo a satisfacción de la suscripción del licenciamiento por doce (12) meses, detallando las labores realizadas. El licenciamiento deberá quedar a nombre del FNA.

• Entregar la matriz de riesgos del proyecto, limitada al alcance de implementación de la solución contratada.

• Entregar la relación de documentos a presentar durante la ejecución del contrato, tales como planes, metodología, cronogramas, guías, manuales y memorias técnicas asociadas a la solución implementada.

• Establecer acciones de mejora y mejores prácticas de uso de la plataforma, sin perjuicio de la entrega de los manuales requeridos en el numeral Plan de Transferencia de Conocimiento y Manuales.

4.4.2 Informes de Gestión

El Contratista deberá presentar un (1) **informe de gestión**, mensualmente y por el plazo de ejecución, dentro de los cinco (5) días hábiles siguientes al vencimiento de cada mes, a partir del inició del servicio de la administración. Este Informe será requisito para el pago de la correspondiente factura del pago recurrente mensual al Contratista.

El informe de gestión deberá detallar entre otras la siguiente información:

- Las labores realizadas durante el periodo del informe.
- Los resultados obtenidos.
- Los reportes del Monitoreo.
- Disponibilidad de la plataforma al corte mensual.
- Métricas e indicadores de cumplimiento frente a las Guías de aseguramiento tecnológico del FNA.
- Gestión de Incidentes, gestión de problemas, entre otros.
- Actividades programadas de soporte por parte del fabricante, hallazgos, acciones realizadas y cambios que se hayan implementado en la plataforma durante el periodo.
- Acciones de mejora que se aplicaron para optimizar la operación de la plataforma.
- Plan de acción de mejoras en la operación.

4.4.3 Informes Soporte Técnico

El soporte técnico que se realice deberá generar un Informe por parte del Contratista y presentarlo al supervisor del contrato, dentro de los cinco (5) días hábiles siguientes a la realización del soporte técnico.

El informe debe deberá considerar entre otros la siguiente información:

- Los procedimientos realizados durante soporte técnico, con el detalle del paso a paso, fechas, horas y acciones
- Gestión de problemas presentados.
- Actualizaciones realizadas.
- Causas identificadas que generen correctivos.
- Acciones de mejora que se aplicaron para optimizar el soporte técnico de la plataforma.

4.4.4 Capacity Planning

El Contratista debe elaborar y entregar el Capacity Planning del nuevo modelo de arquitectura de control de acceso, de acuerdo con las necesidades de la entidad, en el que se realice un análisis y evaluación de la plataforma instalada, incluyendo proyecciones de crecimiento a 12 meses.

Esta entrega deberá efectuarse durante el mes ocho (8) de ejecución del contrato (cuatro meses antes de la terminación), de forma que el FNA pueda tomar decisiones oportunas sobre ampliación de licenciamiento, ajuste de capacidad o renovación contractual.

4.4.5 Gap Final

Un mes antes de la finalización del contrato, el Contratista deberá presentar con el informe de gestión de ese periodo, el Gap Final en el que se encuentren definidas todas las acciones que considere necesarias para cubrir las brechas encontradas en este ejercicio final.

El informe final debe detallar entre otras la siguiente información:

- Resultados finales respecto la administración y soporte.
- Gap final considerando el último mes de servicio.
- Documentos de trabajo que soporten la ejecución de las actividades del cronograma.
- Relación de documentos entregados durante la ejecución del contrato.
- Relación de actualizaciones de manuales de los componentes de la plataforma, así como la entrega de estos de acuerdo con lo requerido en el numeral Plan de transferencia de conocimiento y Manuales.

5 MANTENIMIENTO CORRECTIVO (SOFTWARE)

El Contratista realizará durante la ejecución de contrato, la prestación de los servicios de Mantenimiento Correctivo para la plataforma administrada considerando lo siguiente:

5.1 Mantenimiento Correctivo

Todos los componentes deberán contar con garantía y soporte técnico especializado referente a actualización, instalación, operación y/o configuración básica y atención a cualquier tipo de falla en cualquiera de sus componentes.

En todo caso la garantía de la solución integrada debe ser de fabrica e incluir diagnóstico, remplazo de componentes por fallas en el funcionamiento, suministro e instalación de los respectivos repuestos y mano de obra en sitio (si aplica).

Se deberá realizar en modalidad de (24x7), con un tiempo de respuesta no mayor a cuatro (4) horas por parte del Contratista, y deberá prestarse en las instalaciones en donde se encuentre instalada la plataforma (si aplica), debe incluir:

- El contratista deberá entregar asistencia técnica y oportuna remoto por daños de la plataforma durante la garantía.
- El contratista deberá entregar asistencia técnica con personal calificado para efectuar el diagnostico, reparación y pruebas que se requieran hasta comprobar el buen funcionamiento de la plataforma.
- El contratista deberá realizar la reparación y/o reemplazo de las unidades y/o partes y demás elementos utilizados como parte de la plataforma en caso de daño y/o falla incluyendo la mano de obra necesaria, sin ningún costo adicional para el FNA.
- El contratista deberá realizar un diagnóstico respecto a la falla técnica que presenta la plataforma implica la necesidad de cambiar algún repuesto o parte, éste se efectuará en el lugar donde está instalada la plataforma; de no ser posible, deberá ser reemplazada por otra plataforma de similares o superiores características en calidad de préstamo, sin costo adicional para el FNA mientras se efectúa la reparación.
- Se deberán realizar todos los mantenimientos correctivos a que haya lugar para lo cual, los elementos y piezas a reemplazar, estarán a cargo del Contratista, previa aprobación por parte del supervisor del contrato, siguiendo el procedimiento de la entidad.
- Las unidades y/o partes que sean reemplazadas en los mantenimientos correctivos realizados durante el termino de duración del contrato, deberán ser nuevos, originales y homologados por el fabricante de la plataforma (si aplica).
- En el caso en que cualquier unidad y/o parte reemplazado presente fallas de fabricación, el Contratista deberá hacer efectiva ante el fabricante la garantía y deberá ser reemplazado por otro nuevo de igual o mejor características (si aplica).

6 EQUIPO MÍNIMO DE TRABAJO Y PERFILES TÉCNICOS

PERFIL REQUERIDO 1: GERENTE DE PROYECTO

Cantidad: 1

Formación académica:

Título profesional en Ingeniería de Sistemas, o Ingeniería electrónica, o Ingeniería de Software, o Ingeniería de Telecomunicaciones.

En cualquiera de las carreras acreditadas deberá contar con título de posgrado según núcleo básico de conocimiento de acuerdo (NBC)SINES, en Gerencia de Proyectos, o Dirección y Gestión de Proyectos o Gerencia de proyectos de ingeniería, o en Seguridad de la Información, o en Gerencia de Proyectos de Teleinformática.

Experiencia general:

Mínimo certificado de OCHO (08) AÑOS contada a partir de la expedición de la tarjeta profesional o expedición del título profesional según corresponda.

Experiencia específica:

Mínima certificada en roles de liderazgo, coordinación o de GERENCIA DE PROYECTOS de CUATRO (04) AÑOS contada a partir de la obtención del título profesional en proyectos relacionados con Sistemas de protección o seguridad informática o seguridad de la Información o Ciberseguridad.

PERFIL REQUERIDO 2: INGENIERO SEGURIDAD

Cantidad: 1

Formación académica:

Título profesional en Ingeniería de Sistemas o Ingeniería Informática o Ingeniería Sistemas Informáticos o ingeniería electrónica o Ingeniería de Software o Ingeniería de Telecomunicaciones o similares según NBC del SNIES.

Deberá contar con título de posgrado según núcleo básico de conocimiento de acuerdo (NBC)SINES en Seguridad de la Información, Ciberseguridad, Seguridad en Nube, Gestión de Proyectos, Gestión de Servicios de TI o áreas afines.

Experiencia general:

Mínimo certificado de SIETE (07) AÑOS contada a partir de la expedición de la tarjeta profesional o expedición del título profesional según corresponda.

Experiencia específica:

Mínima certificada de CINCO (5) AÑOS como implementador de proyectos de tecnología o seguridad, responsable de seguridad de la información (CISO), analista de seguridad de la información, o en actividades de diseño o implementación de soluciones de ciberseguridad, en entidades públicas o privadas..

PERFIL REQUERIDO 3: INGENIERO DE SERVICIOS Y SOPORTE

Cantidad: 1

Formación académica:

Título profesional en Ingeniería de Sistemas, o Ingeniería de Sistemas Informáticos, o Ingeniería electrónica, o Ingeniería de Telecomunicaciones.

Deberá contar con título de posgrado según núcleo básico de conocimiento de acuerdo (NBC)SINES en seguridad Informática o Ciberseguridad).

Certificación técnica vigente emitida por el fabricante de la solución ofertada.

Experiencia general:

Mínima de TRES (3) AÑOS en el sector TI contados a partir de la obtención de la tarjeta profesional.

Experiencia específica:

Mínima certificada de TRES (3) AÑOS en cargos relacionados con análisis de seguridad de la información.

REQUISITOS DE ACREDITACIÓN DEL FABRICANTE Y AVAL TÉCNICO DE LA SOLUCIÓN

El proponente deberá acreditar la relación comercial, técnica y de soporte con el fabricante de la solución ofertada, así como el aval técnico correspondiente sobre los componentes incluidos en la propuesta.

Relación comercial y técnica con el fabricante

Se deberá acreditar la relación comercial y técnica activa y vigente con el fabricante de la solución ofertada, en uno de los dos niveles más altos del programa oficial de canales de dicho fabricante. Esta condición debe estar soportada mediante certificado emitido directamente por el fabricante, con fecha de expedición no superior a treinta (30) días anteriores a la presentación de la oferta, en el que conste de forma explícita el nivel de membresía otorgado y su período de vigencia.

No se aceptan certificaciones emitidas por distribuidores, mayoristas o terceros distintos al fabricante, ni documentos sin fecha de vigencia definida.

Aval técnico del fabricante sobre la solución ofertada

El proponente deberá aportar una certificación emitida por el fabricante de la solución ofertada, en la que se relacione la plataforma: navegador seguro para 2500 usuarios con licenciamiento y soporte por 12 meses y servicios profesionales entregados directamente por el fabricante. Esta certificación deberá estar dirigida al FNA e incluir el objeto del proceso y su fecha de expedición no superior a treinta (30) días anteriores a la presentación de la oferta,

7 PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será de Doce (12) meses, contados a partir de la firma del acta de inicio, previo el cumplimiento de los requisitos de perfeccionamiento y ejecución, de los cuales los dos (2) primeros meses corresponden a la instalación, configuración, integración, pruebas, puesta en marcha y estabilización de todos los componentes que hacen parte del nuevo modelo de arquitectura de control de acceso.

8 FORMA DE PAGO

El Fondo Nacional del Ahorro pagará al Contratista el valor del contrato de la siguiente manera:

- **Un pago:** por concepto de suscripción del Licenciamiento, contra entrega del **Certificado de soporte y mantenimiento con fabricante, en modo de suscripción del licenciamiento por 12 meses,** de cada uno de los componentes que hacen parte del nuevo modelo de arquitectura de control de acceso, a nombre del FNA, conforme al valor ofrecido en la oferta económica, previa verificación del apoyo a la supervisión y aprobación por parte del supervisor del contrato.

- **Un pago**: por concepto de la Instalación, configuración, pruebas, puesta en marcha y estabilización de los nuevos componentes que hacen parte del nuevo modelo de arquitectura de control de acceso, contra entrega de cada uno de los entregables definidos para cada uno de estos nuevos componentes, conforme al valor ofrecido en la oferta económica, previa verificación del apoyo a la supervisión y aprobación por parte del supervisor del contrato.

- Se realizarán **pagos por mensualidades vencidas** correspondiente a la administración, Soporte, implementaciones y configuraciones adicionales, gestión de requerimientos y monitoreo continuo de seguridad, los cuales se empezaran a

pagar a partir de la **puesta en operación del nuevo modelo de arquitectura de control de acceso**, conforme al valor ofrecido en la oferta económica y de acuerdo con los servicios efectivamente prestados, previa verificación del apoyo a la supervisión y aprobación de los informes de gestión respectivos por parte del supervisor del contrato.

9 OBLIGACIONES ESPECÍFICAS O CONTRACTUALES DEL CONTRATISTA

1. Cumplir a cabalidad con los requerimientos y especificaciones técnicas señaladas en el Anexo No.1 Especificaciones Técnicas – NAVEGADOR SEGURO que hace parte integral del presente Contrato.
2. Poner a disposición del Fondo Nacional del Ahorro S.A. el equipo de trabajo con los roles y perfiles indicados en el Anexo No.1 Especificaciones Técnicas – NAVEGADOR SEGURO durante la ejecución del contrato.
3. Todo el personal asignado al desarrollo del contrato deberá asistir a la inducción institucional de seguridad de la Información, Sarlaft y conocimiento de producto. Adicionalmente todo el personal asignado al contrato debe contar con cuenta de correo corporativo del dominio asignado por parte del Proponente.
4. Garantizar que el 100% del personal firme un acuerdo de confidencialidad antes de iniciar las labores previas del contrato, este a su vez debe ser compartido al supervisor designado del Fondo Nacional del Ahorro S.A., durante la etapa de implementación y la ejecución del contrato con base en las novedades de personal que se presenten.
5. Responder por las obligaciones que contraiga con el personal empleado para la prestación de los servicios y la realización de los trabajos, por cuanto es entendido que éste no tendrá vinculación con el Fondo Nacional del Ahorro S.A. y toda la responsabilidad derivada de la relación laboral correrá a cargo del Contratista.
6. Renovar e implementar actualizaciones de licenciamiento de las plataformas tecnológicas que hagan parte del objeto del presente proceso con soporte fabricante.
7. Brindar soporte de fabricante y mantenimiento técnico 7X24 por doce (12) meses vía telefónica, correo electrónico y/o conexión remota.
8. Documentar los procesos y las arquitecturas de solución en la herramienta de Arquitectura Empresarial del Fondo Nacional del Ahorro S.A.
9. Disponibilidad para hacer reuniones, sesiones de trabajo y/o de seguimiento con el Fondo Nacional del Ahorro S.A de forma presencial o remota según se requiera.
10. Brindar la debida transferencia de conocimiento cuando se solicite.
11. Presentar para aprobación por parte del Fondo Nacional del Ahorro S.A. la metodología que se utilizará para implementar y renovar, actualizar componentes, transferir conocimiento, administrar y soportar (funcional y técnicamente) la plataforma objeto del presente proceso, especificando etapas, recursos, entregables, herramientas y técnicas a utilizar.

12. Renovar y adquirir contrato de soporte y mantenimiento de fabricante para todos los componentes actuales y nuevos que hacen parte de la plataforma objeto del presente proceso, por doce (12) meses.
13. Cumplir con todas las normas legales sobre aspectos de seguridad de la información emitidas y las que se emitan y que apliquen al Fondo Nacional del Ahorro S.A, durante la vigencia del contrato, y en especial, las que se encuentran en el Anexo No.1 Especificaciones Técnicas
14. Garantizar que permanezcan activados los logs de auditoría de la solución en los cuales se registre toda la actividad administrativa, de mantenimiento y soporte de la solución, y que se mantenga intacta la integridad, confidencialidad y disponibilidad de dichos logs por el tiempo de ejecución del contrato.
15. Cumplir con los entregables transversales del contrato para las fases de inicio, planeación, ejecución del contrato y cierre usando marcos de referencia de Gerencia de Proyectos y metodologías ágiles.
16. Hacer uso de las plantillas establecidas por el Fondo Nacional del Ahorro S.A para la documentación del proyecto sí estas estuviesen disponibles y hacer uso del Manual de Imagen Institucional para todos los entregables y documentos del Contrato.
17. Realizar la medición mensual de los Acuerdos de Niveles de Servicio definidos en el **apartado 10. ACUERDOS DE NIVELES DE SERVICIO – ANS** del presente documento, y establecer los planes de acción correspondientes en caso de presentarse desviaciones, conforme al alcance de la solución contratada y a los ANS previamente validados.
18. Radicar ante el supervisor la factura comercial, acompañada de la certificación de pago de aportes al Sistema de Seguridad Social debidamente suscrita por el Representante Legal o Revisor fiscal, cuando a ello haya lugar, informe de ejecución que para el efecto suscriba el supervisor del contrato donde se verifique el cumplimiento por parte del Contratista respecto de sus obligaciones, y de los demás requisitos exigidos por la Subdirección Administrativa y Financiera. La no presentación de estos documentos o hacerlo en forma extemporánea, exonera al Fondo Nacional del Ahorro S.A. del pago de intereses moratorios.
19. Entregar al supervisor del Fondo Nacional del Ahorro S.A. el Informe de gestión en forma mensual dentro de los cinco (5) días habiles siguientes al vencimiento del mes, en donde se detallen las actividades desarrolladas, el avance y los resultados para el respectivo periodo.
20. Realizar la identificación, tipificación, valoración y asignación de los riesgos que aplican para el presente proceso y realizar seguimiento mensual de los mismos definiendo los planes de acción necesarios para evitar su materialización.
21. Al finalizar la ejecución del contrato, el CONTRATISTA hará entrega formal al supervisor del contrato o quien este delegue, toda la documentación técnica generada o actualizada de las soluciones implementadas y un informe detallado sobre el estado final del proyecto (Gap final). Así mismo, entregará todos los procesos, procedimientos instrumentos de gestión y bases de conocimiento que se desarrollen durante toda la ejecución del contrato.

22. El Contratista deberá garantizar el cumplimiento de los procedimientos administrativos vigentes, establecidos por el Fondo Nacional del Ahorro S.A., respecto al registro de los activos fijos tangibles e intangibles que hagan parte integral del contrato.
23. Ejecutar las demás actividades que sean necesarias o que se requieran a criterio del supervisor para lograr el total y fiel cumplimiento del objeto contractual y las obligaciones, aunque no estén específicamente señaladas en este documento, siempre y cuando las mismas correspondan a la naturaleza y objeto del contrato.

10 ACUERDOS DE NIVELES DE SERVICIO – ANS

- **ANS durante la fase de planeación y diseño:**

  Durante la fase de planeación y diseño, el Contratista deberá entregar los documentos definidos para esta etapa dentro del primer mes de ejecución del contrato.

  El cumplimiento de esta fase se medirá con base en la entrega oportuna de los siguientes documentos:

  - ✓ Plan de trabajo y cronograma

  Plazo: Dentro de los 30 días hábiles de ejecución del contrato.

  El Contratista deberá atender las observaciones documentales realizadas por la Entidad y presentar los ajustes correspondientes dentro de un plazo máximo de cinco días hábiles, contado a partir de la recepción formal de dichas observaciones, siempre que los ajustes dependan directamente del Contratista.

  Cuando la entrega o aprobación de los documentos dependa de información pendiente, definiciones técnicas, accesos, validaciones internas, aprobaciones de la Entidad o participación de terceros, el cronograma podrá ajustarse de común acuerdo entre las partes.

- **ANS durante la fase de implementación y configuración**

  El cumplimiento de esta fase se medirá con la implementación y configuración de la solución conforme al diseño aprobado por la Entidad.

  Plazo: Dentro del 60 días hábiles de ejecución del contrato**.**

  Cuando la entrega o aprobación de los documentos dependa de información pendiente, definiciones técnicas, accesos, validaciones internas, aprobaciones de

la Entidad o participación de terceros, el cronograma podrá ajustarse de común acuerdo entre las partes.

- **ANS generales de soporte**

  El Contratista deberá prestar soporte durante la vigencia contractual para la atención de incidentes, fallas, consultas y solicitudes asociadas a la solución:

ANS general	Tiempo máximo de atención
Incidentes críticos en producción	Hasta 8 horas hábiles
Incidentes no críticos	Hasta 16 horas hábiles
Consultas o solicitudes menores	Hasta 24 horas hábiles
Ajustes de configuración o cambios operativos	Según cronograma acordado con la Entidad
Reportes de estado, disponibilidad, incidencias, cambios y recomendaciones	Mensual
Métricas adicionales de operación y soporte	A proponer por el Contratista, de acuerdo con mejores prácticas y capacidades de la solución

  Los tiempos objetivo aplicarán sobre actividades bajo control directo del Contratista. Cuando la atención dependa de información, aprobaciones, accesos, definiciones técnicas, validaciones internas de la Entidad, terceros, fabricante o disponibilidad de participantes, los tiempos podrán ajustarse conforme al cronograma acordado entre las partes.

- **ANS de disponibilidad para el servicio cloud del Gateway ZTNA**

  Cuando la solución ofertada contemple un modelo de despliegue cloud para el Gateway ZTNA, el servicio cloud administrado por el fabricante deberá contar con una disponibilidad mensual mínima de 99.9%, conforme a la documentación oficial del fabricante.

  Este ANS aplicará únicamente sobre el componente cloud del Gateway ZTNA administrado por el fabricante. No aplicará sobre componentes locales, infraestructura suministrada por la Entidad, conectividad, estaciones de trabajo, certificados, DNS, proveedor de identidad, directorios, aplicaciones privadas publicadas, infraestructura del centro de datos, configuraciones de terceros o servicios externos no administrados por el fabricante.

Componente	ANS	Alcance
Servicio cloud del Gateway ZTNA	≥99.9% de disponibilidad mensual de la solución una vez se encuentre en producción	Aplica únicamente cuando la solución ofertada utilice modalidad cloud para el Gateway ZTNA

Exclusiones del ANS

No se considerarán incumplimientos del ANS de disponibilidad del servicio cloud de ZTNA en los eventos derivados de:

- Ventanas de mantenimiento planificadas por el fabricante.
- Ventanas de mantenimiento de emergencia.
- Motivos de fuerza mayor.
- Fallas de conectividad de la Entidad o de terceros.
- Indisponibilidad del proveedor de identidad, directorio, DNS o certificados.
- Fallas en estaciones de trabajo, agentes, navegadores, aplicaciones privadas publicadas o infraestructura local.
- Cambios no autorizados o configuraciones realizadas por terceros fuera del alcance del Contratista.
- El FNA deberá informar oportunamente al Contratista sobre cualquier cambio programado que pueda impactar la operación de la solución, incluyendo cambios sobre la infraestructura ZTNA, proveedor de identidad, directorio, DNS, certificados, estaciones de trabajo, agentes, navegadores, aplicaciones privadas publicadas o infraestructura local relacionada.
- Los tiempos objetivo de atención aplicarán únicamente sobre actividades bajo control directo del Contratista. Cuando la atención dependa de información, aprobaciones, accesos, definiciones técnicas, validaciones internas de la Entidad, disponibilidad de participantes, terceros, fabricante o componentes administrados por la Entidad, los tiempos podrán ajustarse conforme al cronograma acordado entre las partes.
- El Contratista deberá reportar la disponibilidad en el informe mensual de gestión.

11. MARCO REGULATORIO

El Contratista seleccionado deberá ejecutar el objeto contractual de conformidad con las normas legales sobre seguridad de la información que resulten aplicables al alcance del contrato y, cuando corresponda, apoyar al FNA en su implementación y cumplimiento. Las disposiciones que entren en vigencia durante la ejecución del contrato serán exigibles únicamente en la medida en que resulten aplicables al objeto contractual y no impliquen modificaciones al alcance, las obligaciones, el plazo o el equilibrio económico del contrato, entre las que se encuentran:

- El plan de trabajo debe considerar los lineamientos fijados por las normas y estándares aplicables a la Gestión de la Seguridad de la Información como son las Circulares Externas 029 de 2014, 014 de 2009, 038 de 2009; familia de normas ISO 27000, gestión de riesgos ISO 31000 e ISO 27032 y Políticas de Seguridad de la Información del FNA.
- Circular Externa 029 de 2014: Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios.
- Circular Externa 14 de 2009: Instrucciones relativas a la revisión y adecuación del Sistema de Control Interno (SCI).
- Circulares 007 y 008 de 2018 y 005 del 2019 de la SFC en lo que resulte aplicable al objeto contractual y al alcance de la solución contratada.
- Circular Externa 38 de 2009: Modificación a la Circular Externa 014 de 2009
- Estándares familia ISO 27000
- Ley 1266 de 2008: Ley de Habeas Data
- LEY ESTATUTARIA 1581 DE 2012, Por la cual se dictan disposiciones generales para la protección de datos personales.
- Circular Externa 41 de 2007: Modificación al Capítulo XXIII denominado “Reglas Relativas a la Administración del Riesgo Operativo - SARO” de la Circular Externa 100 de 1995, en lo que resulte aplicable al objeto contractual y a las funcionalidades de la solución, como apoyo al cumplimiento de las obligaciones del FNA.
- Acuerdo 1140 "Manual del Sistema de Control Interno para la Gestión Tecnológica en el FNA". en lo que resulte aplicable al objeto contractual y siempre que dicho documento sea suministrado oficialmente al contratista por el FNA.
- "Manual de Políticas de Seguridad de la Información en el FNA", Vigente en el FNA.
- Circular N° 01 2022: RECOMENDACIONES DE USO DE SERVICIOS EN LA NUBE COMO MEDIDA PARA MITIGAR RIESGOS DE SEGURIDAD DIGITAL de la DIRECTOR DEL DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE

LA REPÚBLICA Y CONSEJERO PRESIDENCIAL PARA LA TRANSFORMACIÓN DIGITAL Y GESTIÓN Y CUMPLIMIENTO.

- DIRECTIVA PRESIDENCIAL 02 DEL 24 DE FEBRERO DE 2022: REITERACIÓN DE LA POLÍTICA PÚBLICA EN MATERIA DE SEGURIDAD DIGITAL DE LA PRESIDENTE DE LA REPÚBLICA.
- Decreto N° 338 2022: "Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto único 1078 de 2015, Reglamentario del Sector de Tecnologías de la información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones". en lo que resulte aplicable al objeto contractual y al alcance de la solución contratada.

Elaboró: Enrique A. Arrázola Montes – Profesional 03

Aprobó: Juan Sebastián Cardenas Hernández - Gerente Ciberseguridad-Aseguramiento Informático