

Ficha técnica
Proceso de Gestión Contractual

- 1. Objeto de la contratación:** Adquirir, instalar, configurar, implementar y soportar una solución integral de ciberseguridad compuesta por: (i) un Firewall de Nueva Generación (NGFW) con prevención avanzada de amenazas, sandboxing y acceso remoto seguro; (ii) una solución de protección de correo electrónico y plataformas de colaboración en la nube; y (iii) una plataforma de gestión centralizada de seguridad en la nube; para fortalecer la seguridad perimetral y la protección de los sistemas de información y usuarios del Departamento Administrativo de la Función Pública
- 2. Lugar de ejecución:** El contratista realizará las actividades propias del objeto en la ciudad de Bogotá D.C, en el Departamento Administrativo de la Función Pública Carrera 6 # 12-62.
- 3. Códigos UNSPSC:** 43201553, 43222501, 43232801, 43233203, 43233204, 81111801, 81111808
- 4. Descripción detallada del bien, servicio u obra a cotizar**

El objeto a cotizar corresponde a la Adquisición, instalación, configuración y puesta en funcionamiento de un appliance de firewall de nueva generación (NGFW), con activación de una suite de seguridad avanzada para protección contra amenazas, la implementación de una plataforma centralizada de gestión y monitoreo de seguridad en la nube, así como los servicios profesionales de migración, configuración e implementación requeridos para la transición desde la plataforma actualmente en operación en el Departamento Administrativo de la Función Pública – DAFP.

El alcance de la contratación comprende los siguientes componentes y servicios:

1. Appliance de seguridad de propósito específico con suscripción a servicios avanzados de protección por un (1) año: incluye funcionalidades de firewall de nueva generación (NGFW), sistema de prevención de intrusiones (IPS), protección anti-bot, antivirus, filtrado de URLs, control de aplicaciones, inspección de tráfico HTTPS/TLS, emulación de amenazas (sandboxing), protección contra phishing y conectividad VPN (site-to-site y acceso remoto);
2. Plataforma de gestión centralizada basada en la nube por un (1) año: administración de dispositivos de seguridad con capacidad para hasta 3 GB de registros diarios y retención de 3 meses, incluyendo módulo de correlación y análisis de eventos de seguridad;



Función Pública

3. Suscripción a funcionalidades SD-WAN por un (1) año: habilitación de capacidades de SD-WAN sobre el appliance base;
4. Ocho (8) transceptores SFP 1G de corto alcance (1000Base-SX): para la conexión de puertos de fibra óptica del appliance con la infraestructura de red del DAFP;
5. Licencia de acceso remoto seguro ilimitado por un (1) año: acceso remoto seguro mediante SSL VPN sin restricción de usuarios concurrentes;
6. Suscripciones de software empresarial y soporte premium por un (1) año: para el appliance y los módulos SD-WAN, que incluyen actualizaciones de software, parches de seguridad y soporte del fabricante;
7. Servicio profesional de implementación y migración: diseño, configuración, migración de políticas desde la solución de seguridad anterior (hasta 1.000 reglas de firewall, objetos de red y políticas NAT), configuración de hasta dos (2) VPNs site-to-site, validación del despliegue, transferencia de conocimiento y documentación técnica;
8. Solución de protección de correo electrónico y plataformas de colaboración en la nube, entregada como servicio SaaS para quinientos treinta (530) usuarios y buzones por un (1) año: protege el correo corporativo en Office 365 y/o Google Workspace, así como las plataformas Slack, Microsoft Teams, OneDrive, SharePoint, Google Drive, Box, Dropbox y Citrix ShareFiles. Incluye, como mínimo: prevención de phishing, BEC, spoofing y spam mediante motores de Inteligencia Artificial y Machine Learning con análisis de metadatos, adjuntos, códigos QR e historial de comunicaciones; integración nativa por API con Office 365 y/o Google Workspace sin modificar registros MX; protección antimalware basada en firmas y análisis estático; sandboxing resistente a la evasión con veredicto en no más de cinco (5) minutos y emulación en entornos Windows; limpieza de documentos (CDR – Content Disarm and Reconstruction); rescritura e inspección de URLs en tiempo de clic incluyendo adjuntos y códigos QR; detección de cuentas comprometidas (account takeover) con bloqueo automático; detección y reporte de Shadow IT; portal de gestión con control de acceso basado en roles (RBAC), tableros en tiempo real y exportación de eventos en formatos CSV, JSON y XLSX; integración con SIEM vía syslog TCP o JSON sobre HTTP y soporte de API REST; retención de correos en cuarentena y metadatos de eventos maliciosos por mínimo ciento ochenta (180) días; disponibilidad del servicio SaaS de al menos 99,9%, con certificación SOC 2 o ISO 27001 vigente; y reconocimiento como solución líder en seguridad de correo electrónico por analistas independientes de tercer nivel en los últimos tres (3) años. Incluye servicio profesional de implementación, configuración, integración con el directorio corporativo, migración de políticas de la solución actual y validación en producción.

5. Naturaleza técnica del bien o servicio a contratar El bien y servicio a contratar es de naturaleza tecnológica mixta, compuesto por:

- A. Bien tecnológico – Hardware: appliance físico de seguridad perimetral (Firewall de Nueva Generación) en formato mínimo 1U Rack Mount, para instalación en el Data Center del DAFP, con capacidad de throughput de 40 Gbps en modo firewall y 20 Gbps en modo NGFW, destinado a reemplazar el equipo actualmente en operación como dispositivo de seguridad perimetral principal de la entidad;
- B. Suscripciones de software de seguridad: licenciamiento anual de una suite de seguridad avanzada, plataforma de gestión centralizada basada en la nube, funcionalidades SD-WAN, acceso remoto seguro y soporte premium del fabricante; uso esperado: protección del perímetro de red, control de acceso a internet, prevención de amenazas avanzadas, gestión centralizada de políticas de seguridad y acceso remoto seguro mediante VPN para los funcionarios y sistemas del DAFP.
- C. Servicios profesionales especializados: implementación, migración de plataforma, transferencia de conocimiento.

6. Plazo de ejecución del contrato: 3 Meses.
Plazo para suscripciones y garantía: 1 año

7. Especificaciones técnicas

Campo de identificación técnica	ÍTEM	DESCRIPCIÓN	Cant.	Tiempo de entrega con implementación (bien/servicio)	Tiempo de suscripción
1. Firewall	1	Appliance de seguridad de propósito específico con suscripción a servicios avanzados de protección por 1 año, de acuerdo con el numeral 2. CARACTERISTICAS DEL HARDWARE Y REDIMIENTO DE LA SOLUCIÓN de la hoja	1	45 días calendario siguientes al inicio de la ejecución del contrato, para la entrega de los equipos objeto del contrato	N/A dado que es la adquisición del componente físico.



Función Pública

		especificaciones técnicas del equipo.			
	2	Transceptor SFP para puertos de fibra óptica 1G de corto alcance (1000Base-SX), compatible con appliances de seguridad de distintas series y modelos.	8	45 días calendario siguientes al inicio de la ejecución del contrato, para la entrega de los equipos objeto del contrato	N/A dado que es la adquisición del componente físico.
	3	Suscripción de plataforma de gestión centralizada basada en la nube para administrar el gateway, con capacidad para hasta 3 GB de registros diarios y retención de 3 meses por 1 año, incluyendo módulo de correlación y análisis de eventos de seguridad.	1	15 días calendario siguientes a la entrega de los equipos objeto del contrato	1 año desde la entrega y recibo a satisfacción
	4	Suscripción a funcionalidades SD-WAN por 1 año para el appliance de seguridad base. Habilito enrutamiento dinámico basado en políticas, monitoreo de enlaces y selección de rutas según calidad de servicio, gestionable desde una plataforma centralizada de administración local o en la nube.	1	15 días calendario siguientes a la entrega de los equipos objeto del contrato	1 año desde la entrega y recibo a satisfacción
	5	Licencia de acceso remoto seguro ilimitado por 1 año. Permite acceso remoto seguro	1	15 días calendario siguientes a la entrega de los	1 año desde la entrega y recibo a satisfacción



Función Pública

		mediante VPN SSL (en modo portal y modo túnel) sin restricción de usuarios concurrentes. Compatible con autenticación multifactor y Single Sign-On.		equipos objeto del contrato	
	6	Suscripción de software empresarial y soporte premium para el equipo de seguridad por 1 año. Incluye actualizaciones del sistema operativo, parches de seguridad y soporte técnico del fabricante 24x7, con acceso a portal de atención al cliente.	1	15 días calendario siguientes a la entrega de los equipos objeto del contrato	1 año desde la entrega y recibo a satisfacción
	7	Suscripción de software empresarial y soporte premium para la plataforma de gestión centralizada por 1 año. Incluye soporte premium, actualizaciones de la consola de administración y del módulo de correlación y análisis de eventos de seguridad.	1	15 días calendario siguientes a la entrega de los equipos objeto del contrato	1 año desde la entrega y recibo a satisfacción
	8	Suscripción de software empresarial y soporte premium para el módulo adicional de SD-WAN por 1 año. Incluye soporte premium sobre la suscripción de SD-WAN, actualizaciones de funcionalidades y soporte especializado del fabricante	1	15 días calendario siguientes a la entrega de los equipos objeto del contrato	1 año desde la entrega y recibo a satisfacción
	9	Preproducción e Implementación	1	15 días calendario	N/A dado que es un servicio



Función Pública

	• Configurar hasta 1 plataforma de gestión centralizada en la nube. • Configurar hasta 1 GW, 1 clúster • Integración entre el nuevo GW/Clúster/Grupo de Seguridad con el sistema de gestión. • Convertir hasta 1 política de la plataforma (hasta 1000 reglas). - Objetos de red. - Reglas de firewall. - Políticas de NAT. • Importar la política. • Configurar hasta 2 VPNs de sitio a sitio. • Validar que el despliegue fue exitoso. Traspaso de producción: • Soporte para el traspaso y puesta en marcha fuera del horario laboral. Transferencia de conocimientos: • Transferencia y entrega de conocimientos. Documentación • Elaborar un cuestionario para confirmar los requisitos de conectividad y el diseño propuesto. • Método de procedimiento detallado: un documento que describe todo el proceso de instalación con cada comando y paso de configuración utilizado en la implementación. • Hoja de aprobación/verificación	siguientes a la entrega de los equipos objeto del contrato	de implementación
--	--	---	--------------------------



Función Pública

		que garantiza la instalación según las mejores prácticas del fabricante.			
2. Sw de filtrado de correo	10	Solución de protección de correo electrónico y plataformas de colaboración en la nube, entregada como servicio SaaS para quinientos treinta (530) usuarios y buzones por un (1) año: protege el correo corporativo en Office 365 y/o Google Workspace, así como las plataformas Slack, Microsoft Teams, OneDrive, SharePoint, Google Drive, Box, Dropbox y Citrix ShareFiles. Incluye, como mínimo: prevención de phishing, BEC, spoofing y spam mediante motores de Inteligencia Artificial y Machine Learning con análisis de metadatos, adjuntos, códigos QR e historial de comunicaciones; integración nativa por API con Office 365 y/o Google Workspace sin modificar registros MX; protección antimalware basada en firmas y análisis estático; sandboxing resistente a la evasión con veredicto en no más de cinco (5) minutos y emulación en entornos Windows; limpieza de documentos (CDR – Content Disarm	1	15 días calendario siguientes a la entrega de los equipos objeto del contrato	1 año desde la entrega y recibo a satisfacción



Función Pública

		and Reconstruction); reescritura e inspección de URLs en tiempo de clic incluyendo adjuntos y códigos QR; detección de cuentas comprometidas (account takeover) con bloqueo automático; detección y reporte de Shadow IT; portal de gestión con control de acceso basado en roles (RBAC), tableros en tiempo real y exportación de eventos en formatos CSV, JSON y XLSX; integración con SIEM vía syslog TCP o JSON sobre HTTP y soporte de API REST; retención de correos en cuarentena y metadatos de eventos maliciosos por mínimo ciento ochenta (180) días; disponibilidad del servicio SaaS de al menos 99,9%, con certificación SOC 2 o ISO 27001 vigente; y reconocimiento como solución líder en seguridad de correo electrónico por analistas independientes de tercer nivel en los últimos tres (3) años. Incluye servicio profesional de implementación, configuración, integración con el directorio corporativo, migración de políticas de la solución actual y validación en producción.			
--	--	---	--	--	--

8. Actividades a desarrollar:

Las actividades a desarrollar en el marco del presente contrato son las siguientes:

1. **ALISTAMIENTO Y PREPRODUCCIÓN:** El contratista deberá realizar el levantamiento de información sobre la infraestructura actual del DAFP (topología de red, políticas de seguridad vigentes en equipo actual, VPNs activas, reglas NAT, objetos de red), a fin de elaborar el diseño técnico de la solución propuesta y el plan detallado de migración. Se deberá entregar al supervisor del contrato, dentro de los primeros cinco (5) días hábiles contados desde la suscripción del acta de inicio, el documento de diseño de arquitectura y el cronograma de implementación.
2. **INSTALACIÓN FÍSICA DEL APPLIANCE:** Instalación física del appliance de seguridad en el rack del Data Center del DAFP (Carrera 6 N° 12-62, Bogotá D.C.), conforme a las especificaciones del fabricante. Incluye la conexión de los puertos de red (RJ-45 y SFP) a la infraestructura de switching existente, la instalación de los ocho (8) transceptores SFP 1G y la verificación de la conectividad física.
3. **CONFIGURACIÓN E IMPLEMENTACIÓN:** Configuración inicial del sistema operativo de seguridad, activación de licencias y suscripciones a servicios avanzados de protección (como prevención de amenazas, SD-WAN y acceso remoto seguro), configuración del servidor de gestión centralizada en la nube, integración del gateway con la plataforma de administración y configuración de los parámetros de red (interfaces, VLANs, rutas, alta disponibilidad si aplica).
4. **MIGRACIÓN DE POLÍTICAS DESDE EQUIPO ACTUAL:** Conversión y migración de hasta mil (1.000) reglas de la plataforma actualmente en producción al nuevo ambiente de seguridad, incluyendo: objetos de red (hosts, grupos, subredes), reglas de firewall, políticas de NAT y configuración de hasta dos (2) VPNs site-to-site. La migración deberá validarse en un ambiente de preproducción antes del paso a producción.
5. **ACTIVACIÓN DE MÓDULOS DE SEGURIDAD:** Activación y configuración de los módulos de seguridad incluidos en la suscripción avanzada: sistema de prevención de intrusiones (IPS), protección anti-bot, antivirus, filtrado de URLs, control de aplicaciones, emulación de amenazas (sandboxing), protección contra

phishing, inspección de tráfico HTTPS/TLS (capas 1-7) y acceso remoto seguro mediante VPN SSL.

6. **TRASPASO A PRODUCCIÓN:** Soporte durante la ventana de cambio a producción (fuera del horario laboral, previa coordinación con el supervisor del contrato), incluyendo el corte del tráfico desde la plataforma existente hacia el nuevo appliance de seguridad, verificación funcional de todos los servicios críticos del DAFP y plan de reversión (rollback) en caso de incidencias.

7. **DOCUMENTACIÓN TÉCNICA:** Entrega de los siguientes documentos al supervisor del contrato como condición previa para la suscripción del acta de recibo a satisfacción:

- i Documento de diseño de arquitectura as-built de la solución implementada;
- ii Procedimiento detallado de implementación con comandos y pasos de configuración utilizados;
- iii Hoja de verificación y aprobación de instalación conforme a mejores prácticas de fabricante;
- iv Inventario de licencias y fechas de vencimiento de suscripciones.

8. **TRANSFERENCIA DE CONOCIMIENTO:** El contratista deberá realizar una sesión de transferencia de conocimiento dirigida al equipo de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) del Departamento Administrativo de la Función Pública – DAFP, con una duración mínima de 8 horas, en modalidad presencial o virtual. Dicha sesión deberá llevarse a cabo antes de la suscripción del acta de recibo definitivo del contrato y cubrirá, como mínimo, los siguientes aspectos: arquitectura implementada, consola de gestión centralizada, gestión de políticas de firewall, módulos de prevención de amenazas, diagnóstico de vpn, revisión de logs y alertas y procedimientos de contingencia.

8. Condiciones de garantía:

Plazo garantía	Alcance de la garantía	Procedimiento para hacer efectiva	Procedimiento técnico para reponer bienes defectuosos
Un (1) año contado a partir de la suscripción del acta de inicio	Hardware (appliance de seguridad): garantía de reemplazo de partes	1. El supervisor del contrato reporta el incidente al contratista por	Para hardware (appliance de seguridad): el contratista



Función Pública

del contrato y activación de los productos.	defectuosas o del equipo completo por parte del fabricante durante la vigencia del contrato, en caso de falla física. Suscripciones de software (servicios avanzados de protección, gestión centralizada en la nube, SD-WAN, acceso remoto seguro, soporte premium): incluyen actualizaciones	correo electrónico o canal de soporte acordado. 2. El contratista acusa recibo en un plazo máximo de dos (2) horas hábiles. 3. Para incidentes críticos (pérdida total de conectividad o falla del firewall), el tiempo de respuesta técnica inicial será de máximo cuatro (4) horas. Para incidentes no críticos, máximo veinticuatro (24) horas hábiles. 4. Si el soporte remoto no resuelve el incidente, el contratista deberá desplazar ingeniero certificado a la sede	gestionará el proceso de RMA (Return Merchandise Authorization) ante el fabricante y suministrará un equipo de reemplazo con características iguales o superiores. El reemplazo deberá realizarse a costo del contratista, incluyendo la instalación, configuración y restauración de las políticas en funcionamiento, en un plazo máximo de cinco (5) días hábiles desde la apertura del caso de soporte. Para suscripciones de software: el contratista
---	--	---	--

9. Requisitos técnicos del personal mínimo requerido:

- Ingeniero implementador de la solución**

Perfil técnico del personal	Personal mínimo requerido	Experiencia general y específica	Porcentaje de dedicación cuando aplique
Profesional en Ingeniería de Sistemas o electrónica o informática o afines, y Especialista en seguridad de la información.	Un (1) ingeniero certificado por el fabricante.	4 años de experiencia general desde la obtención de título y 1 año en gestión de proyectos de ciberseguridad en la marca ofertada.	100%

- El Personal requerido no es un requisito técnico habilitante, sin embargo, este se deberá acreditar conforme a la ficha técnica respecto de los perfiles, formación académica y experiencia, mediante la entrega de la documentación y soportes correspondientes con anterioridad al inicio del cronograma de actividades y el supervisor deberá dejar evidencia de la revisión y aprobación del personal. En caso de requerir el reemplazo de algún profesional o técnico, informar al supervisor con mínimo cinco (5) días hábiles de anticipación y garantizar que la persona propuesta acredite igual o mayor nivel de formación, experiencia y certificaciones que las exigidas en la ficha técnica para el respectivo rol. El reemplazo solo podrá efectuarse previa aprobación escrita del supervisor, so pena de requerimiento y aplicación de las medidas previstas en el contrato por incumplimiento de obligaciones contractuales.

Responsabilidades: Implementar todas las fases del proyecto: diseño, preproducción, implementación, migración, puesta en producción y transferencia de conocimiento. Ejecutar la migración de políticas desde la plataforma actual hacia la nueva solución de seguridad, garantizando la continuidad operativa del DAFP. Configurar y validar la integración con la plataforma de gestión centralizada en la nube. Atender las solicitudes de soporte durante la implementación., bajo demanda del supervisor del contrato. Elaborar y entregar la documentación técnica completa (as-built, procedimiento de implementación, hoja de verificación). Realizar la sesión de transferencia de conocimiento al equipo de la OTIC del DAFP.

10. Cronograma de ejecución:

Entregar dentro de los cinco (5) días hábiles siguientes a la suscripción del acta de inicio, el cronograma de trabajo detallado, con identificación de actividades, duraciones, responsables, ventanas de mantenimiento requeridas, diagrama de arquitectura propuesta (before/after) y rollback plan para el traspaso a producción. Dicho plan deberá ser aprobado por el supervisor antes del inicio de cualquier actividad de implementación.

11. Requisitos técnicos:

En relación con los requisitos técnicos requeridos, estos se encuentran definidos en el estudio previo en los requisitos habilitantes técnicos numeral 13.3 el cual hace parte integral del proceso.

12. Garantías del contrato

El contratista se obliga a constituir, a favor de Departamento Administrativo de la Función Pública, una Garantía de cumplimiento dentro de los cinco días hábiles siguientes del perfeccionamiento del contrato, de conformidad con lo establecido en el artículo 2.2.1.2.3.1.2 del Decreto 1082 de 2015 expedida por una compañía de seguros o entidad bancaria legalmente autorizada para ello, con el fin de respaldar todas las obligaciones que surjan del mismo, con los siguientes amparos:

De acuerdo con lo establecido en el artículo 7 de la Ley 1150 de 2007, el numeral 7 del artículo 2.2.1.1.2.1.1. y el Libro 2, Parte 2 Capítulo I, Sección 3 del Decreto 1082 de 2015, **EL CONTRATISTA** deberá amparar los riesgos derivados de la presente contratación, de conformidad con la siguiente tabla:

AMPARO	%	SOBRE EL VALOR	VIGENCIA
Cumplimiento del contrato	20%	Valor total del contrato	Por el plazo de ejecución del contrato, y doce meses (12) más, contados a partir de la suscripción del contrato. Cubrirá los perjuicios derivados de: i. Incumplimiento total o parcial del contrato, cuando el incumplimiento es imputable al contratista; ii. El cumplimiento tardío o defectuoso del contrato, cuando éste es imputable al

			contratista. iii. El pago del valor de las multas y de la cláusula penal pecuniaria. Nota: En todo caso deberá estar vigente hasta la liquidación del contrato de conformidad con el artículo 2.2.1.2.3.1.12. Suficiencia de la garantía de cumplimiento del Decreto 1082 del 2015.
Calidad y correcto funcionamiento de los bienes	20%	Valor total del contrato	Por el término de un (1) año, contado a partir del recibo a satisfacción por parte del supervisor del bien, previa entrega, instalación y puesta en funcionamiento,
Calidad del servicio	20%	Valor total del contrato	Por el término de ejecución del contrato y un (1) año más, contado a partir de la suscripción del contrato.
Pago de salarios, prestaciones sociales legales e indemnizaciones laborales	10%	Valor total del contrato	Igual al plazo de ejecución del contrato y tres (3) años más, contados a partir de la suscripción del contrato.

Nota 1. El hecho de la constitución de estos amparos no exonera a la entidad de las responsabilidades legales en relación con los riesgos asegurados. El contratista deberá mantener vigentes las garantías a que se refiere este numeral y mantener la suficiencia de las mismas. Será de su cargo el pago de todas las primas y demás erogaciones de constitución, mantenimiento y restablecimiento inmediato de su monto, cada vez que se disminuya o agote por razón de las sanciones que se impongan, prórrogas o suspensiones.

Nota 2. El contratista deberá realizar todas las gestiones necesarias para mantener vigentes las garantías o seguros a que se refiere esta cláusula.

Nota 3. Estará a cargo del contratista el pago de la prima y demás erogaciones de constitución y mantenimiento de las garantías mencionadas.

Nota 4. En caso de que el contrato se adicione, prorrogue o suspenda o cualquier otro evento que fuera necesario, el contratista se obliga a modificar las pólizas señaladas en esta cláusula, de acuerdo con las normas legales vigentes.

Nota 5. La garantía única de cumplimiento expedida a favor de entidades públicas no expirará por falta de pago de la prima ni podrá ser revocada unilateralmente, según se preceptúa en el Artículo 2.2.1.2.3.2.5 del Decreto 1082 de 2015.

Nota 6. A la entidad estatal no le serán oponibles por parte del asegurador las excepciones o defensas provenientes de la conducta del tomador del seguro, en especial las derivadas de las inexactitudes o reticencias en que este hubiere incurrido con ocasión de la contratación del seguro ni en general, cualesquiera otras excepciones que posea el asegurador en contra del contratista.

Nota 7. Para efectos de constituir las garantías el contratista deberá tener en cuenta el valor del contrato, dentro de la misma deberá contener como mínimo la siguiente información (vigencia, tomador / afianzado, número del contrato, objeto).

Nota 8. Cuando la oferta es presentada por un proponente plural, como unión temporal o consorcio, la garantía debe ser otorgada por todos sus integrantes e indicar el porcentaje de participación de cada uno de ellos.

Nota 9. La garantía de cumplimiento deberá contar con la Constancia de No Revocatoria o el comprobante de pago de la misma.

16. OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA

1. Ejecutar la totalidad de las actividades descritas en el objeto del contrato y en la ficha técnica, respetando las especificaciones técnicas, los estándares normativos aplicables y las instrucciones del supervisor del contrato. Ninguna actividad podrá omitirse, reducirse en alcance ni sustituirse por una alternativa diferente sin autorización escrita previa del supervisor.
2. Suscribir el acta de inicio dentro de los tres (3) días hábiles siguientes al perfeccionamiento del contrato.
3. Entregar dentro de los cinco (5) días hábiles siguientes a la suscripción del acta de inicio, el cronograma de trabajo detallado, con identificación de actividades, duraciones, responsables, ventanas de mantenimiento requeridas, diagrama de arquitectura propuesta (before/after), transferencia de conocimiento y la documentación de estas sesiones y rollback plan para el traspaso a producción. Dicho plan deberá ser aprobado por el supervisor antes del inicio de cualquier actividad de implementación.
4. Realizar, previo al inicio de la implementación, un levantamiento conjunto con el supervisor del estado actual de la infraestructura existente del DAFP, incluyendo el inventario de políticas activas, objetos de red, reglas NAT, VPNs site-to-site configuradas y configuraciones de VPN SSL. Cualquier incompatibilidad técnica, riesgo identificado o condición anómala deberá reportarse al supervisor por escrito antes de proceder. La omisión de este reporte implicará que el contratista asume responsabilidad sobre las afectaciones no reportadas.

5. Instalar, configurar y poner en funcionamiento el appliance propuesto en el Data Center de la entidad, incluyendo: instalación física en rack, conexión de interfaces con transceptores SFP 1G SX adquiridos, configuración del sistema operativo de seguridad del fabricante ofertado, activación y registro de licencias a nombre del DAFP en el portal de la solución propuesta, integración y configuración inicial de consola de administración.
6. Activar y configurar la totalidad de los módulos de seguridad avanzada incluidos en la suscripción de prevención de amenazas del fabricante ofertado: IPS, Antivirus, Anti-Bot, Filtrado de URLs, Control de Aplicaciones, Inspección HTTPS/TLS (capas 1-7), emulación de amenazas (Sandboxing), protección anti-phishing avanzada, módulo de acceso remoto seguro VPN SSL. Cada módulo deberá quedar con las políticas base alineadas a las necesidades del DAFP, validadas y aprobadas por el supervisor del contrato.
7. Migrar las políticas de seguridad desde la plataforma existente actualmente en operación hacia la nueva plataforma propuesta, garantizando la migración de reglas de firewall, objetos de red y políticas NAT, así como la configuración de VPNs site-to-site. La migración deberá realizarse en un ambiente de preproducción y ser validada funcionalmente por el supervisor antes del traspaso definitivo a producción.
8. Coordinar con el supervisor del contrato, con mínimo veinticuatro (24) horas de anticipación, cada ventana de mantenimiento requerida para intervenciones que impliquen impacto en la conectividad a internet o servicios del DAFP. El traspaso final a producción deberá realizarse fuera del horario laboral (antes de las 7:00 a.m. o después de las 6:00 p.m., o en fin de semana), con acompañamiento del supervisor o quien este delegue, y con el rollback plan disponible para ejecución inmediata en caso de falla.
9. Configurar y activar la suscripción SD-WAN y el módulo de acceso remoto seguro VPN SSL ilimitado en el appliance, incluyendo la configuración de políticas de acceso remoto VPN SSL (modo Portal y modo Túnel) para los usuarios del DAFP, con integración al directorio de usuarios institucional (Active Directory) si aplica, según instrucción del supervisor.
10. Activar, configurar e integrar la plataforma de gestión centralizada en la nube al gateway implementado, con retención de logs de hasta 3 GB diarios y 3 meses de retención, y habilitar el módulo de correlación y análisis de eventos de seguridad. El contratista deberá entregar al supervisor las credenciales de administración y la guía de acceso a la consola.
11. Acreditar el personal requerido en la ficha técnica respecto de perfiles, formación académica y experiencia, mediante la entrega de la documentación y soportes correspondientes con anterioridad al inicio del cronograma de actividades y el supervisor deberá dejar evidencia de la revisión y aprobación del personal. En caso de requerir el reemplazo de algún profesional o técnico, informar al supervisor con

mínimo cinco (5) días hábiles de anticipación y garantizar que la persona propuesta acredite igual o mayor nivel de formación, experiencia y certificaciones que las exigidas en la ficha técnica para el respectivo rol. El reemplazo solo podrá efectuarse previa aprobación escrita del supervisor, so pena de requerimiento y aplicación de las medidas previstas en el contrato por incumplimiento de obligaciones contractuales.

12. Realizar la sesión de transferencia de conocimiento al equipo de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) del DAFP, con una duración mínima de ocho (8) horas, presencial o virtual, cubriendo como mínimo: arquitectura implementada, administración de la consola de gestión centralizada en la nube, gestión de políticas de firewall, operación de los módulos de prevención de amenazas avanzadas, diagnóstico de VPN, revisión de logs y alertas de eventos, y procedimientos de contingencia. La sesión deberá realizarse antes de la suscripción del acta de recibo definitivo.
13. Entregar la documentación técnica completa como condición previa para la suscripción del acta de recibo definitivo, incluyendo: (a) Documento as-built con diagrama de arquitectura final, interfaces configuradas, segmentos de red, VLANs y configuración de alta disponibilidad si aplica; (b) Inventario de licencias y suscripciones activadas a nombre del DAFP con fechas de vencimiento; (c) Procedimiento detallado de administración y operación cotidiana; (d) Registro de políticas migradas con matriz de equivalencia (e) Certificado del fabricante propuesto acreditando las suscripciones activadas a nombre del DAFP. Toda la documentación deberá entregarse en medio digital editable y en PDF
14. Suscribir con el supervisor del contrato el acta de recibo a satisfacción como condición previa para el trámite del pago y el cierre del contrato, en la que se certifique el cumplimiento total del objeto contractual, la correcta instalación y funcionamiento de la solución implementada, la revisión, verificación y aprobación de la totalidad de los bienes adquiridos conforme a las especificaciones técnicas de la ficha técnica, y la entrega completa de la documentación técnica requerida. El pago no podrá tramitarse sin la suscripción previa de dicha acta, debidamente firmada por el contratista y el supervisor del contrato.
15. Garantizar la continuidad operativa del DAFP durante toda la ejecución del contrato. El contratista responderá directamente ante el DAFP por cualquier interrupción de servicios de conectividad a internet, VPN o seguridad perimetral que sea consecuencia directa de una acción u omisión de su personal, y deberá restablecer el servicio en un plazo máximo de seis (6) horas a partir de la notificación del supervisor, sin perjuicio de las demás acciones contractuales y legales a que haya lugar.
16. El contratista durante la ejecución del contrato deberá propender por mantener las buenas prácticas de seguridad de la información a través de controles de

confidencialidad, integridad, disponibilidad, gestión de accesos, manejo seguro de credenciales, protección de la información de la entidad, atención de incidentes y cumplimiento de los lineamientos de seguridad definidos por la entidad; para todo lo cual deberá acreditarlo con los soportes correspondientes.

17. Entregar los bienes dentro de los cuarenta y cinco (45) días calendario siguientes al perfeccionamiento y legalización del contrato, y dejar la solución totalmente instalada, configurada, activa y en operación, incluida la activación y registro de todas las suscripciones y licencias dentro de los quince (15) días calendario siguientes a la entrega del equipo.

OBLIGACIONES GENERALES DEL CONTRATISTA

1. Cumplir con el objeto contratado, de acuerdo con las especificaciones requeridas por el Departamento Administrativo de la Función Pública.
2. Presentar los informes que el Departamento Administrativo de la Función Pública solicite sobre su gestión y en desarrollo del objeto contractual.
3. Atender con prontitud y efectividad las solicitudes, condiciones y/o recomendaciones que dentro de los términos del Contrato el Supervisor del mismo establezca.
4. Cumplir con la normativa vigente, en materia ambiental aplicable al objeto contractual, con lo cual se contribuye a la política ambiental establecida por el Departamento Administrativo de la Función Pública y es responsable de los daños, perjuicios, pérdidas y siniestros que a nivel ambiental se ocasionen debido a alguna acción, retardo, omisión o negligencia suya o de sus subcontratistas.
5. Constituir las garantías que se establecen en este contrato.
6. No acceder a peticiones o amenazas de quienes actúen por fuera de la Ley, con el fin de obligarlos a hacer u omitir cualquier acto o hecho.
7. Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones y entramamientos que puedan presentarse y en general se obliga a cumplir con lo establecido en la ley 80 de 1993, la ley 1150 de 2007, sus reformas y decretos reglamentarios.
8. Responder por sus actuaciones y omisiones derivadas de la celebración del contrato y de la ejecución del mismo, de conformidad con lo establecido en la Ley 80 de 1993.
9. Acreditar el pago de sus obligaciones frente al Sistema Integral de Seguridad Social en Salud, Pensión y Riesgos Laborales, así como los propios del Sena, ICBF y Cajas de Compensación Familiar, de conformidad con lo establecido en el inciso 3º del artículo 50 de la ley 789 de 2002 y demás normas vigentes, presentando los soportes de pago correspondientes, anexos al informe de actividades con el fin de tramitar cada pago.

10. Cumplir con la obligación de afiliación y cotización al Sistema de Seguridad Social Integral (salud, pensiones y riesgos laborales) del personal contratado para la ejecución del contrato.
11. Desarrollar e implementar su política en SST y gestionar los riesgos que son objeto de la negociación bajo un Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST). Cumplir con los estándares mínimos en Seguridad y Salud en el Trabajo establecidos en la Resolución 0312 de 2019 y/o las que la modifiquen según normatividad vigente, incluyendo Estándares Mínimos para trabajadores en actividades de alto riesgo de acuerdo con los que hace referencia el artículo 31 de la Resolución citada, si es el caso del objeto del Contrato. PARÁGRAFO: Aportar dentro de los siguientes 20 días calendario siguientes a la firma del Acta de Inicio del contrato: -Documento con la Identificación de peligros y valoración de riesgos vigente. -Documento que contenga Plan Anual de Trabajo del Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST) firmado por el empleador o contratante, en el que se identifiquen como mínimo: objetivos, metas, responsabilidades, recursos y cronograma anual de la vigencia. PARÁGRAFO 2. El DAFP se reserva el derecho a verificar durante la ejecución del contrato el cumplimiento de estos requisitos de acuerdo con el Decreto 1072 de 2015, en su artículo 2.2.4.6.28, el cual establece: “Artículo 2.2.4.6.28 Contratación. El empleador debe adoptar y mantener las disposiciones que garanticen el cumplimiento de las normas de seguridad y salud en el trabajo de su empresa, por parte de los proveedores, trabajadores dependientes, trabajadores cooperados, trabajadores en misión, contratistas y sus trabajadores o subcontratistas, durante el desempeño de las actividades objeto del contrato
12. Fomentar la vinculación y mantener durante la ejecución del contrato recurso humano en condición de extrema pobreza, desplazados por la violencia, personas en proceso de reintegración y sujetos de protección constitucional, en un porcentaje que no sea superior al 10% ni inferior al 5% del total de los bienes y servicios requeridos para la ejecución del contrato, esta obligatoriedad será verificada por el supervisor del contrato. de conformidad del artículo 3 del Decreto 1860 de 2021 que adicionó el artículo 2.2.1.2.4.2.16., del Decreto 1082 de 2015 (Cuando aplique).
13. PREVENCIÓN Y DENUNCIA DE LA VIOLENCIA BASADA EN GÉNERO. Prevenir, corregir y denunciar, ante las autoridades administrativas y/o las autoridades judiciales correspondientes, según sea el caso, la violencia, la discriminación, el abuso y el acoso sexual contra las mujeres, y las demás violencias basadas en género, lo anterior en cumplimiento del CONPES 4080 de 2022: “Política pública de equidad de género para las mujeres: hacia el desarrollo sostenible del país”; el Protocolo de Prevención, Atención y Medidas de Protección contra todas las formas de Violencia, expedido por el Departamento Administrativo de la Función Pública, Versión 1, de fecha Septiembre de 2025, desarrollado en cumplimiento de la

Directiva Presidencial 001 de 2023 y la Ley 2365 de 2024, por la cual se adoptan medidas de prevención, protección y atención del acoso sexual en el ámbito laboral y en las instituciones de educación superior en Colombia

14. **ELIMINACIÓN DEL LENGUAJE SEXISTA.** Evitar los elementos de discriminación sexista en el uso del lenguaje escrito, visual, audiovisual y de la imagen, que perpetúen estereotipos de género y/o generen un ambiente sexual hostil, prácticas discriminatorias y estereotipos de género y racistas.
15. Las demás obligaciones inherentes a la naturaleza del contrato, que sean necesarias para el cumplimiento de este según el pliego de condiciones, sus anexos y adendas, así como la propuesta presentada por EL CONTRATISTA

OBLIGACIONES DEL DAFP

1. Expedir el Registro Presupuestal una vez se suscriba el contrato objeto del proceso.
2. Aprobar las garantías del contrato en caso de que aplique.
3. Suscribir, en caso de que aplique, en conjunto con el contratista, el acta de inicio del contrato y demás actas que se requieran durante la ejecución del contrato.
4. Suministrar al contratista la información clara y oportuna que se requiera para la ejecución del contrato.
5. Designar el supervisor del contrato, que se encargue de ser el enlace entre el DAFP y el contratista para coordinar las actividades propias del contrato.
6. Verificar el cumplimiento de las obligaciones previstas en la Ley 100 de 1993 y sus decretos reglamentarios, en el artículo 50 de la Ley 789 de 2002, leyes 828 de 2003, 1122 de 2007, 1150 de 2007 y 1562 de 2012 y demás normas concordantes.
7. Realizar a través del supervisor del contrato el seguimiento técnico, administrativo, financiero, sobre el cumplimiento del objeto del contrato y efectuar los requerimientos que estime pertinentes.
8. Expedir las certificaciones de cumplimiento a satisfacción para los pagos correspondientes una vez estas hayan sido aprobadas por el supervisor.
9. Ejercer las facultades y cumplir los deberes establecidos en la Ley 1474 de 2011 y los contenidos en la Ley 80 de 1993.
10. Realizar el pago del valor del contrato en las condiciones pactadas.
11. Responder oportunamente las solicitudes presentadas por el contratista dentro del término de ejecución del contrato, previo el análisis que deba realizar sobre la procedencia y viabilidad en la solicitud o circunstancia expuesta. Teniendo especial cuidado en que no opere el silencio administrativo positivo.
12. Para el correspondiente pago, la factura presentada por el contratista aceptado, acompañadas de las certificaciones de cumplimiento a satisfacción, el documento soporte del pago de aportes parafiscales relativos al Sistema de Seguridad Social

Integral, así como los propios del Sena, ICBF y Caja de Compensación Familiar, ARL.

13. Adelantar oportunamente los trámites requeridos para la programación del PAC correspondiente a los pagos a que haya lugar.
14. Terminado el plazo de ejecución del contrato elaborar el informe final de ejecución.
15. En general todas las que se desprendan del ejercicio de la supervisión.

Nombre quien diligencia: David Arturo Sánchez Mendoza

Dependencia: Oficina de Tecnologías de la Información y las Comunicaciones