SECRETARIA DISTRITAL DE SALUD FONDO FINANCIERO DISTRITAL DE SALUD
ANEXO TÉCNICO OBJETO

1. OBJETO

Adquirir una solución integral de ciberseguridad incluyendo la instalación, configuración, soporte y garantía de soluciones avanzadas de ciberseguridad para fortalecer la infraestructura digital de la Secretaría Distrital de Salud.

2. ALCANCE DEL OBJETO

Adquirir las soluciones necesarias, junto con su licenciamiento y soporte, para robustecer la infraestructura de ciberseguridad de la Secretaría Distrital de Salud. La implementación incluirá la instalación y configuración conforme a las especificaciones del anexo técnico, aplicando las mejores prácticas del fabricante y asegurando su integración efectiva con las soluciones perimetrales existentes dentro del ecosistema Security Fabric, el cual permite una operación coordinada, automatizada e integral para la protección de la infraestructura digital institucional.

3. SOLUCIONES A SUMINISTRAR

3.1. SOLUCIÓN DE BALANCEO DE CARGA

Tabla 1 Solución de balanceo de carga

ITEM	REQUERIMIENTO TECNICO MINIMO DE OBLIGATORIO CUMPLIMIENTO
1	La solución deberá proveer balanceo de carga de aplicaciones (ADC) en capas 4 y 7.
2	El dispositivo debe ser un equipo de propósito específico. La solución deberá estar compuesta por un componente ADC y un componente de seguridad (integrado o incluido como un módulo del ADC o independiente con integración nativa).
3	Los componentes podrán ser dispositivos físicos independientes o integrados en un mismo appliance. Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux. La solución debe ser desarrollada por el mismo fabricante y no debe incluir desarrollos de terceros.
4	La solución deberá operar en alta disponibilidad (HA), activo-activo o activo-pasivo. Se deben incluir dos equipos en HA.
5	Todos los componentes deberán contar con soporte oficial del fabricante.
6	Rendimiento mínimo capa 4: 40 Gbps.
7	Rendimiento mínimo capa 7: 30 Gbps.
8	Rendimiento SSL acorde al dimensionamiento de la solución.
9	Debe incluir mínimo 30 servicios o dominios virtuales
10	Debe incluir Interfaces suficientes para soportar los enlaces de la entidad, como mínimo con puertos 10 Gbps SFP+.
11	Balanceo de tráfico TCP, UDP e IP.
12	Soporte de protocolos: HTTP, HTTPS, RADIUS, SIP, DNS, FTP, SMTP.

ITEM	REQUERIMIENTO TECNICO MINIMO DE OBLIGATORIO CUMPLIMIENTO
13	Métodos de balanceo: round robin, weighted round robin, least connections, Fastest response.
14	Persistencia de sesión basada en IP origen, cookies, SSL session ID y hash.
15	Health checks configurables: ICMP, TCP, HTTP, HTTPS.
16	Selección de servidor basada en URL, headers HTTP y cookies.
17	Reescritura de cabeceras HTTP.
18	Compresión HTTP (GZIP o equivalente).
19	Caché HTTP (o equivalentel).
20	Soporte de políticas o scripting para manejo de tráfico.
21	Soporte de TLS 1.2 y TLS 1.3.
22	Capacidad de SSL offloading.
23	Reutilización de sesiones SSL.
24	Perfiles de cifrado configurables.
25	La solución deberá incluir o permitir integración nativa con componente de seguridad.
26	El componente de seguridad deberá incluir firewall stateful, IPS y protección DDoS.
27	Soporte de inspección de tráfico cifrado SSL/TLS.
28	Integración con inteligencia de amenazas y sandbox mediante APIs estándar.
29	Interoperabilidad entre ADC y seguridad mediante APIs estándar o integración nativa o conectores.
30	Soporte de IPv4 e IPv6.
31	Soporte de VLANs, NVGRE y VXLAN.
32	Soporte de NAT, NAT64 y NAT46.
33	soporte de BGP y OSPF o equivalente.
34	Failover automático.
35	Sincronización de configuración entre nodos.
36	La solución debe integrarse con la solución de logs y reportes de la entidad, ya sea vía API estándar, conector o syslog
37	Interfaz gráfica (GUI).
38	Interfaz de línea de comandos (CLI).
39	API REST.
40	Monitoreo mediante SNMP y syslog.

3.2. SOLUCIÓN DE ANÁLISIS DE MALWARE

Tabla 2 Solución de análisis de malware

ITEM	REQUERIMIENTO TÉCNICO MÍNIMO
1	La solución debe ser del tipo appliance físico de propósito específico
2	La Solución no debe ser de tipo en-línea (inline), no se acepta ninguna solución que agregue más puntos de falla y latencia en la red o demoras en las trasferencias de los archivos
3	Los componentes que integran la solución no deben aparecer en listas end-of-life ó end-of-sale del fabricante.
4	La solución deberá contar con API por medio del método RESTful sobre HTTPS.
5	El contratista deberá realizar un análisis de la arquitectura de red actual, con el fin de aplicar las mejores prácticas para la implementación.
6	La solución debe contar con soporte técnico y retorno de hardware por parte del fabricante por un periodo de un (1) año en un esquema 7 x 24 incluyendo actualizaciones de firmware, acceso al portal de soporte y recursos técnicos asociados. Los incidentes técnicos podrán ser reportados vía web, chat y teléfono

ITEM	REQUERIMIENTO TÉCNICO MÍNIMO
7	La solución deberá soportar múltiples máquinas virtuales para la ejecución simultánea de análisis dinámico, con un mínimo de 15 instancias concurrentes o superior.
8	La solución deberá permitir equivalencia o benchmarking
9	La solución deberá tener un rendimiento mínimo de análisis estático de 30.000 archivos por hora o superior
10	La solución deberá tener un rendimiento mínimo de análisis dinámico de 600 archivos por hora o superior
11	La solución deberá poder ejecutar de código malicioso en sistemas operativos virtuales.
12	La solución deberá contar con múltiples técnicas de análisis previas a la ejecución en sandbox, incluyendo como mínimo análisis antivirus, consultas a servicios de inteligencia de amenazas (locales o en la nube) y mecanismos de análisis estático, heurístico o de emulación de código.
13	La solución debe contar con un módulo para la importación de reglas YARA.
14	La solución debe estar en la capacidad de detectar los siguientes tipos de infección y ataques: Gusanos, Botnet, Hijack, Stealer, Backdoor, Injector, RootKit, Adware, Troyanos, Riskware, Greayware.
15	Toda la clasificación (Maliciosos, alto, medio, bajo riesgo) deben ser presentados en un dashboard intuitivo.
16	La solución debe presentarse información completa del análisis de amenazas del ambiente virtual incluyendo Actividades del sistema, acción del exploit, trafico web, intentos de comunicación entre otros.
17	La solución deberá contar con capacidades de detección y mitigación de técnicas de evasión utilizadas por malware, incluyendo mecanismos para identificar comportamientos como retrasos en ejecución (sleep), consultas al entorno del sistema (procesos, registros, sistema operativo) y otras técnicas de evasión de sandbox.
18	La solución deberá contar con técnicas de detección de modificación de Archivos, comportamiento de procesos, comportamiento de registros, comportamientos de red.
19	La solución deberá contar con técnicas de detección de callbacks: Visitas a URL maliciosas, Comunicaciones con servidores de comando y control (C&C) y todo el tráfico generado desde la muestra de malware.
20	La solución deberá soportar múltiples sistemas operativos virtuales para análisis dinámico, incluyendo como mínimo Windows, Linux y Android. Se valorará soporte adicional para otros sistemas operativos como macOS o entornos industriales (ICS).
21	Las máquinas virtuales basadas en Windows deberán contar con el licenciamiento correspondiente, ya sea incluido o provisto por la entidad.
22	La solución deberá contar la capacidad de contar con número de clones por cada tipo de máquina virtual debe poder ser parametrizable a criterio de la entidad.
23	La solución debe mostrar los paquetes de software instalados en cada tipo de Máquina Virtual.
24	La solución debe permitir crear listas negras y listas blancas.
25	La solución debe permitir seleccionar que tipos de archivos serán analizados en cada máquina.
26	La solución debe permitir que el usuario cree sus propios tipos de archivos.
27	Debe soportar como mínimo los siguientes tipos de Archivos: .7z, .cmd, .com, .dll, .doc, .docm, .docx, .exe, .gif, .gz, .htm, html, .jpeg, .jpg, .js, .jsp, .mp3, .mp4, .msg, .msi, .pdf, .ppt, .pptm, .pptx, .rar, .tar, .tgz, .txt, .xls, .zip.
28	La solución deberá ser capaz de analizar archivos provenientes de diferentes protocolos de red, incluyendo como mínimo HTTP(S), SMTP, FTP y servicios de correo (POP3/IMAP), ya sea mediante captura de tráfico (modo pasivo/sniffer) o integración con soluciones de seguridad perimetral (ej. NGFW, correo, proxy).
29	La solución deberá soportar el análisis de tráfico cifrado (SSL/TLS) cuando sea proporcionado por dispositivos de seguridad integrados.
30	La solucion deberá enviar de forma automática los archivos catalogados como maliciosos al laboratorio del fabricante para creación y distribución de firmas.
31	La solución debe incluir un módulo de webfiltering para inspeccionar y marcar las conexiones a URL maliciosas que traten de hacer los procesos ejecutados por los archivos que se inspeccionan.
32	Los archivos que son analizados con el OS Sandbox deben entregar un análisis posterior a la ejecución de las siguientes características: Descarga de Virus, Modificación de registro, Conexiones externas a IPs maliciosas, Infección de procesos.
33	La solución debe estar en la capacidad de procesar múltiples archivos al mismo tiempo, se debe contar con múltiples VM para el análisis de Sandbox OS.
34	El resultado de los análisis debe clasificar los archivos de acuerdo al nivel de riesgo como Alto, medio o bajo.

ITEM	REQUERIMIENTO TÉCNICO MÍNIMO
35	Esta clasificación se hará de acuerdo a un score y la cantidad de puntos que tenga cada archivo en su análisis.
36	La solución debe ser posible habilitar él envió de notificaciones cada vez que el análisis detecte archivos maliciosos.
37	File Input: Debe ser posible manualmente hacer una subida de los archivos a analizar.
38	Sniffer: El equipo debe estar en la capacidad de recoger el tráfico de un puerto en modo espejo.
39	- Integración con Firewall de Nueva Generación: En este modo la solución debe integrarse con los NGFW ofertados a la entidad para que estos le envié archivos sospechosos para el análisis.
40	- Integración con la solución ADC: La solución debe integrarse para mejorar las capacidades de análisis antivirus del ADC.
41	Se debe poder implementar en un ambiente distribuido donde múltiples dispositivos de seguridad perimetral le envían archivos para análisis.
42	Soporte de rutas estáticas.
43	Autorización de dispositivos que quieren enviar archivos para análisis.
44	Reportes detallados en características y comportamiento. Modificación de archivos, comportamiento de procesos, comportamiento de registros, comportamientos de red.
45	La solución debe tener reportes en línea en tiempo real, esta debe poder ser personalizable con widgets que se puedan agregar o quitar.
46	Se deben presentar estadísticas de TOP N, con datos de los hosts atacados, malware, URLs, Call Back Domains. Estas estadísticas pueden ser vistas en línea con la posibilidad de seleccionar el período de tiempo que se quieren ver.
47	La solución debe estar en la capacidad de enviar reportes semanalmente.
48	La solución debe entregar online información específica de los análisis realizados, esto debe ser sobre una interfaz gráfica con filtros predeterminados como eventos, malware, entre otros.
49	La información del análisis debe poder ser descargada en un log para en posterior análisis.
50	La solución debe ser posible descargar un archivo PCAP para revisar el comportamiento del archivo.
51	En los casos que aplique debe ser posible descargar un pantallazo de las acciones graficas del archivo sospechoso.
52	La solución deberá integrarse con plataformas de reportería y/o SIEM mediante mecanismos estándar como API REST, syslog, exportación de logs u otros métodos de interoperabilidad.
53	La solución deberá incluir el diseño de la arquitectura y políticas de acuerdo a las necesidades de la entidad y su implementación y puesta en funcionamiento.
54	La solución será responsabilidad del proveedor hasta la aceptación formal de recepción por parte de la entidad.
55	El personal que ejecute los servicios de implementación, configuración y soporte de la solución debe ser certificado por el respectivo fabricante. Este requerimiento será satisfecho con la presentación de las hojas de vida de cada persona y las certificaciones que soporten su habilidad al supervisor de contrato, al momento de su adjudicación.
56	La oferta debe contemplar e incluir el suministro de todos los elementos físicos tal como SFP, SFP+, QSFP, fibras ópticas, cables UTP de acuerdo a la cantidad de puertos establecidos en las especificaciones técnicas, tarjetas, software, licenciamiento, soporte y garantía necesarios para la instalación, interconexión, configuración, puesta en producción, integración de la infraestructura, servicios de migración y servicios profesionales, sin que esto genere costos adicionales para la entidad.

3.3. SOLUCIÓN DE MONITOREO DE INFRAESTRUCTURA

ITEM	REQUERIMIENTO TÉCNICO
1	La entidad requiere un servicio de monitoreo de la experiencia digital (DEM) en modalidad SaaS, que permita la visibilidad del rendimiento de las aplicaciones desde la perspectiva del usuario final, independientemente de su ubicación o del entorno donde se encuentren desplegadas las aplicaciones. Debe ser una herramienta de propósito específico licenciada y con soporte de fábrica, no se aceptan soluciones opensource
2	La solución debe tener la capacidad de monitorear red, usuarios, servidores y servicios, permitiendo la evaluación de aplicaciones de extremo a extremo.

ITEM	REQUERIMIENTO TÉCNICO
3	La solución debe proporcionar visibilidad integral del desempeño de aplicaciones, servicios, red e infraestructura subyacente, permitiendo el análisis de la experiencia digital de manera unificada.
4	La solución debe contar con capacidades de detección temprana de incidentes, correlación de eventos y soporte para la gestión y remediación oportuna de problemas que impacten la experiencia del usuario final.
5	La solución debe realizar monitoreo desde el usuario final hasta los sistemas que soportan las aplicaciones críticas, en entornos locales, híbridos o en nubes públicas o privadas.
6	La solución debe permitir la integración con herramientas de gestión de incidentes, automatización y plataformas de seguridad mediante APIs, conectores o estándares abiertos, con el fin de optimizar los procesos de diagnóstico y remediación.
7	La solución debe incluir capacidades de monitoreo sintético para evaluar disponibilidad, tiempos de respuesta y desempeño de aplicaciones desde la perspectiva del usuario.
8	La solución debe identificar degradaciones en el servicio y generar alertas proactivas.
9	La solución debe correlacionar métricas de aplicaciones, CPU, memoria, disco y red para facilitar la identificación de causas raíz de incidentes.
10	La solución debe soportar el monitoreo del desempeño de redes WAN y SD-WAN mediante técnicas activas y/o pasivas, incluyendo métricas como latencia, pérdida de paquetes, jitter y disponibilidad.
11	La solución debe permitir la integración con dispositivos y plataformas de seguridad para la recolección de métricas de desempeño y estado, mediante mecanismos estándar.
12	La solución debe contribuir a la optimización de los tiempos de detección y respuesta, apoyando el cumplimiento de los SLA definidos por la entidad.
13	La solución debe incluir el monitoreo de al menos 200 dispositivos, entre servidores, equipos de red o dispositivos finales.
14	La solución debe incluir el monitoreo de al menos 200 contenedores, permitiendo evaluar su desempeño y disponibilidad.
15	La solución debe soportar la ejecución de transacciones sintéticas mediante scripts, APIs o herramientas compatibles con navegadores o protocolos estándar, desde ubicaciones públicas o privadas.
16	La solución debe incluir capacidades de descubrimiento automático y mapeo de topología de red, permitiendo visualizar relaciones entre componentes y facilitar la identificación de problemas.
17	El oferente debe incluir servicios de implementación y adopción de buenas prácticas, los cuales podrán ser prestados directamente por el fabricante o por un partner autorizado o certificado.
18	La solución debe integrarse como mínimo con herramientas de colaboración y gestión como Jira, Slack y Microsoft Teams, o equivalentes.
19	La solución debe contar con un dashboard unificado y personalizable para la visualización de métricas, eventos e indicadores clave.
20	La solución debe ser agnóstica respecto a fabricantes, permitiendo monitorear dispositivos de red, aplicaciones, servicios en la nube y plataformas SaaS de múltiples proveedores.
21	La solución debe permitir el envío y escalamiento de alertas a través de múltiples canales como correo electrónico, aplicaciones móviles, SMS, llamadas o integración con sistemas de gestión de tickets.
22	La solución debe permitir la integración con entornos de nube pública, incluyendo al menos AWS y Azure, mediante mecanismos estándar.
23	La solución debe soportar descubrimiento automático de dispositivos mediante protocolos estándar como SNMP u otros equivalentes.
24	La solución debe permitir el monitoreo de entornos de virtualización y orquestación de contenedores, incluyendo tecnologías como VMware y Kubernetes.
25	La solución debe incluir capacidades de automatización mediante plantillas, scripts o flujos de trabajo, orientadas a reducir tareas repetitivas y mejorar los tiempos de respuesta ante incidentes.
26	La solución debe ser compatible e integrable con soluciones tecnológicas existentes en la entidad mediante estándares abiertos, APIs o mecanismos documentados.

3.4. SOLUCIÓN PARA LA PROTECCIÓN DE CORREO ELECTRONICO

ITEM	REQUERIMIENTO TÉCNICO MÍNIMO
1	La solución debe analizar dinámicamente el 100% de los correos electrónicos correspondientes a las dos mil seiscientas (2.928) cuentas de correo institucional incluidas en el alcance, mediante técnicas avanzadas de

ITEM	REQUERIMIENTO TÉCNICO MÍNIMO
	análisis de amenazas que permitan detectar y bloquear malware, phishing, enlaces maliciosos y ataques avanzados, garantizando la protección de las comunicaciones electrónicas de la Entidad.
2	La solución debe analizar todas las URL y archivos adjuntos de los correos electrónicos entrantes
3	La solución debe escanear dinámicamente los correos electrónicos en tiempos adecuados que no afecten la experiencia del usuario.
4	La solución debe tener la capacidad de acceder automáticamente a los detalles del análisis para ver las razones exactas por las que se marca un correo electrónico como malicioso
5	La solución debe proteger activamente contra el spam
6	La solución debe identificar amenazas después de la entrega de correo. Debe estar en capacidad de notificar a los usuarios y recuperar correos electrónicos maliciosos de sus bandejas de entrada para ponerlos en cuarentena automáticamente
7	La solución debe utilizar fuentes de inteligencia sobre amenazas para identificar amenazas conocidas
8	La solución debe utilizar capacidades avanzadas de detección e investigación de amenazas.
9	La solución debe escanear los correos electrónicos de forma estática utilizando motores Antivirus
10	La solución debe utilizar herramientas para identificar firmas muy complejas
11	La solución debe proteger contra los ataques de phishing a través del reconocimiento de imágenes, el análisis de texto y los evaluadores de reputación
12	La solución debe proteger como mínimo contra los ataques BEC cuando se realizan comprobaciones SPF, DKIM y DMARC
13	La solución debe proteger contra los ataques de suplantación de identidad mediante el uso de técnicas para descubrir la suplantación de nombres de visualización y la suplantación de VIP
14	La solución debe proteger contra ataques de día cero y día N mediante técnicas avanzadas de análisis dinámico y comportamiento.
15	La solución debe hacer clic y escanear activamente las direcciones URL para identificar enlaces maliciosos antes de que lleguen al buzón del usuario final
16	La solución debe contar con tecnología Sandbox para identificar archivos maliciosos
17	La solución debe utilizar técnicas avanzadas de análisis del comportamiento para inspeccionar el flujo de ejecución de archivos.
18	La solución debe mantener la integridad de los archivos durante los análisis, evitando alterar la estructura de los archivos
19	La solución debe identificar vulnerabilidades de daño en la memoria
20	La solución debe detectar errores lógicos y macros dentro de los documentos
21	La solución debe escanear cientos de tipos de archivos diferentes
22	La solución debe descomprimir el contenido de forma recursiva, buscando enlaces y archivos incrustados para escanear
23	La tecnología de la solución para escanear enlaces y archivos incrustados debe contar con capacidad de análisis profundo de múltiples niveles.
24	La solución debe analizar contenido protegido con contraseña al entregarse el password
25	La solución debe analizar archivos comprimidos/comprimidos
26	La solución debe ser una plataforma reconocida en el mercado de seguridad de correo electrónico.
27	La solución debe ser nativa de la nube y está totalmente alojada en la nube
28	La solución debe actualizarse automáticamente
29	La solución debe satisfacer las necesidades de escalamiento de licenciamiento de un cliente sin afectar la experiencia del usuario ni requerir la compra de equipos adicionales
30	La solución debe permitir la implementacion en modo de prevención de amenazas, evitando las amenazas antes de que lleguen a los usuarios finales

ITEM	REQUERIMIENTO TÉCNICO MÍNIMO
31	La solución debe permitir ser implementada en modo CCO/Journaling, así como en línea para una protección completa en M365 como mínimo
32	La solución debe permitir la implementacion para los usuarios a través de una invitación por correo electrónico
33	La solución debe ser implementada automáticamente con la integración de Office 365 y/o Google Mail
34	La solución debe tener la posibilidad de conectarse a través de API a otras aplicaciones
35	La solución debe integrarse como mínimo con Office 365 a través de API, gateway o mecanismos equivalentes, sin requerir cambios obligatorios en el registro MX.
36	La solución debe poderse ajustar a las politicas y SIEM existentes y no requiere cambios en la infraestructura e integración via REST APIs
37	La solución debe contar como mínimo con la capacidad de exportar registros en tiempo real al SIEM
38	La solución debe estar en capacidad de integrarse con gestores de Identidades a través de SAML
39	Los usuarios se deben asignan automáticamente permisos a roles y grupos en función de un esquema RBAC
40	La solución debe estar en capacidad mediante licencias adicionales de proteger el uso del cliente del almacenamiento compartido, las herramientas de colaboración y el navegador
41	La solución debe cifrar los datos en reposo con AES-256 y en tránsito con TLS 1.2+
42	Las claves de cifrado deben estar protegidas mediante servicios de gestión de claves (KMS) o mecanismos equivalentes.
43	La solución debe cumplir como mínimo con: SOC2, GDPR, HIPAA, ISO 27001
44	La solución debe estar alojada en múltiples regiones geográficas para garantizar alta disponibilidad y resiliencia del servicio.
45	La solución debe proporcionar un panel de administración informativo que muestre datos de incidentes, informes y políticas
46	La solución debe tener la opcion de incluir en las listas negras o blancas en función de la IP, las URL, los dominios, los remitentes, los tipos de archivos, etc.
47	La solución debe registrar las acciones del usuario, como los intentos de inicio de sesión, los cambios en el veredicto, la publicación de correos electrónicos y las solicitudes de investigación
48	El cliente debe estar en capacidad de personalizar los banners y las alertas de advertencia y traducirlos a otros idiomas como español, inglés y portugues
49	La solución debe tener una forma que el usuario reporte un presunto falso positivo o falso negativo para que la solución la revise y de su veredicto
50	La solución debe enviar informes y resúmenes de acciones a los usuarios
51	La solución debe ofrecer soporte al cliente y capacitación ilimitados según sea necesario sin cargo adicional durante la duracion del contrato
52	La solución debe ser compatible mínimo con Microsoft 365, incluyendo Exchange Online, Microsoft Teams, OneDrive y SharePoint.
53	La solución debe detectar y bloquear archivos maliciosos, URLs maliciosas, phishing y ataques avanzados en el correo electrónico y en los servicios de Microsoft 365 protegidos.
54	La solución debe permitir el análisis y evaluación de correos electrónicos, archivos y URLs intercambiados a través de Exchange Online y los servicios de Microsoft 365 incluidos en el alcance.
55	La solución debe escanear el tráfico de correo electrónico y los archivos almacenados y compartidos dentro del entorno Microsoft 365 protegido.

3.5. SOLUCIÓN DE ACCESO A LA RED (NAC)

ITEM	CONTROL DE ACCESO A LA RED (NAC)
1	Se requiere de una solución de NAC basada en dos (2) appliance físico dedicado, con un paquete de licenciamiento en suscripción para controlar mínimo 3000 dispositivos.
2	La solución debe estar en capacidad de gestionar como mínimo 3000 suscripciones dispositivos concurrentes, con posibilidad de escalabilidad.

ITEM	CONTROL DE ACCESO A LA RED (NAC)
3	La solución deberá ser suministrada mediante appliance físico o virtual para despliegue on-premise, no se aceptan soluciones en nube.
4	El dimensionamiento del appliance deberá ser validado por el fabricante, garantizando el soporte de la cantidad de dispositivos y sesiones requeridas, así como la escalabilidad futura.
5	La solución NAC debe incluir los siguientes bloques funcionales:
6	Visibilidad de red y perfilado de dispositivos conectados.
7	Automatización del proceso de provisión de red en función del tipo de dispositivo que se esté conectando
8	OnBoarding de nuevos dispositivos sencillo, versátil y potente.
9	Endpoint Compliance: Permitiendo a la organización desplegar políticas asociadas a diferentes grupos de usuarios, verificando su cumplimiento y notificando las desviaciones, permitiendo configurar diferentes protocolos de remediación, desde acciones de aislamiento inmediatas a simples notificaciones, pasando por acciones diferidas.
10	Identificación de amenazas, a través de la integración con otros elementos, y ejecución de acciones de remediación en función del evento.
11	Gestión de invitados y usuarios externos: Fácil y rápida, sin necesidad de involucrar al personal de IT en el alta de nuevos usuarios externos por medio de patrocinadores o Sponsors.
12	La solución NAC debe ser agnóstica respecto a los fabricantes del equipamiento de acceso, tanto cableado como inalámbrico y por tanto válida en redes hetereogéneas.
13	La solución NAC debe estar integrada con los dispositivos de red y seguridad existentes, y los que se incluyan en la nueva arquitectura.
14	Debe ser capaz de trabajar bien con agentes instalados en los endpoints, o bien sin agentes.
15	La solución debe soportar múltiples mecanismos de control de acceso, incluyendo 802.1X y RADIUS, sin depender exclusivamente de estos.
16	En caso de ofrecer appliance físico, debe contar con fuentes de poder redundantes hot-plug, que garanticen la continuidad operativa ante fallas eléctricas, conforme a las mejores prácticas del fabricante.
17	La solución debe tener incluidos los modulos de integracion con terceros
18	La solución debe integrarse con las soluciones de seguridad perimetral de la entidad mediante APIs, estándares abiertos o mecanismos certificados por el fabricante.
19	La solución NAC debe tener capacidad para inventariar todos los dispositivos de la red, incluyendo equipamiento que no sea PC, como impresoras, Smartphones (Iphone, Android y Windows Phone), teléfonos IP, cámaras y otros dispositivos IoT que pudieran existir (biométricos…) y dispositivos OT.
20	Debe poder utilizar múltiples métodos de identificación (mínimo 10 o más), tales como DHCP fingerprint, escaneo activo o pasivo, Vendor OUI, ubicación, puertos o información obtenida a través de agentes.
21	HTTP/HTTPS, SSH u otros mecanismos seguros, incluyendo interacción mediante scripts personalizados.
22	Debe incluir un servicio dinámico de identificación de dispositivos IoT que comparta la información disponible sobre el dispositivo a perfilar con un servicio en Nube, que emplee técnicas de inteligencia que ayuden a la identificación del dispositivo.
23	La solución debe soportar como mínimo el perfilado de dispositivos Windows pertenecientes al dominio mediante WMI o WINRM, utilizando canales seguros y validados mediante certificado.
24	La solución debe permitir conectarse a la red corporativa solo a dispositivos autenticados/registrados, desplegando políticas de seguridad que bloqueen y aíslen dispositivos que no cumplan los criterios corporativos, enviándolos a un área de cuarentena sin necesidad de intervención por parte de los administradores de red.
25	La solución debe ser capaz de autorizar los accesos mediante asignación dinámica de VLAN's y/o aplicando ACLs al puerto de acceso.
26	La solución debe ser capaz de controlar escenarios en los que hay más de un equipo conectado a un puerto, asociando a cada equipo la VLAN adecuada, siempre que el equipo de acceso lo permita.
27	La solución debe ser capaz de integrarse con los firewalls para asociar los dispositivos a reglas de seguridad concretas, en función del tipo de dispositivo.
28	La solución debe permitir extender las políticas de seguridad al acceso VPN, ya sea SSL en modo túnel o IPSEC a través de una política de seguridad consistente.

ITEM	CONTROL DE ACCESO A LA RED (NAC)
29	La solución debe soportar autenticación de máquina y usuarios, y como mínimo pudiendo autenticar un endpoint sin usar agentes.
30	La solución debe de ser capaz de asociar al dispositivo atributos adicionales, como la ubicación, tipo de dispositivo, fabricante… además de los atributos del usuario conectado.
31	La solución debe soportar opciones de autenticación flexibles, incluyendo como mínimo 802.1X, autenticación WEB y autenticación MAC.
32	Para despliegues 802.1X, debe poder actuar como Radius Proxy y como Radius local
33	La solución debe soportar integración LDAP y Microsoft Active Directory, sin necesitar ningún componente adicional, para desplegar políticas en función de su pertenencia a ciertos grupos.
34	La solución debe soportar RADIUS Identity store.
35	La solución debe soportar la detección y perfilamiento de sistemas operativos chrome
36	La solución debe contar Integración de MDM incluida
37	La solución debe soportar enforcement por medio de SSH/SNMP
38	La solución debe soportar inspección de los dispositivos tanto basada en agente (persistente y disoluble) como sin agente.
39	La solución NAC debe ser capaz de realizar, al menos, las siguientes comprobaciones: service packs, nivel de parcheo, que haya instalado las actualizaciones críticas, Antivirus y AntiSpyware, servicios y procesos, certificados, existencia de archivos y cualquier entrada del registro de Windows.
40	La solución debe contar con un motor de correlación de eventos.
41	La solución debe proporcionar un rol de cuarenta que se interactúe con los Sistemas de parcheo. De esta manera, los dispositivos corporativos que no cumplan los requisitos serán enviados a un portal cautivo de “autoremediación”: Los equipos que no tengan cumplimiento debe de ser enviados a cuarentena dinámicamente, y o bien se le proporcionan instrucciones para la remediación o se ejecuta la remediación automática mediante integración con herramientas de gestión de parches o administración de endpoints.
42	El Sistema de control de acceso debe proporcionar una plataforma flexible y eficiente de gestión de usuarios no corporativos, que permita manejar el acceso de aquellos usuarios con un acceso transitorio (típicamente invitados) o con un acceso más estable (contratistas externos).
43	La solución debe permitir definir perfiles limitados que solo tengan acceso a la gestión de cuentas de invitados.
44	La solución debe permitir altas masivas (p.e. para conferencias), autoregistros, registros esponsorizados o dados de alta por un administrador.
45	La solución debe permitir autenticaciones por medio de redes Sociales.
46	La solución debe permitir la opcion de aceptar invitados por medio de patrocinadores o Sponsors.
47	La solución debe ser flexible y permitir la definición de diferentes perfiles, como invitados de corta /larga estancia, asistentes a conferencias o auto-registrados.
48	El sistema de control de acceso almacena información crucial sobre la red, cuántos elementos hay conectados y sus características, cuántos cumplen la política de seguridad de la empresa … así como los eventos de seguridad que se puedan haber producido. También almacena información sobre eventos en la red (cambios en los puertos, conexiones…) que pueden ser de gran utilidad para realizar investigaciones después de que se produzca una investigación.
49	La solución debe ofrecer una consola de monitorización, reporting y troubleshooting que ayude a los administradores y operadores de helpdesk.
50	La consola debe ser accesible a través de una GUI Web, sin necesidad de aplicaciones específicas.
51	Debe permitir obtener, al menos, la siguiente información:
52	* Eventos de conexión a lo largo del tiempo
53	* Cambios en los puertos.
54	* Eventos de seguridad detectados por la plataforma a lo largo del tiempo (por ejemplo, fingerprints que cambian, intentos de impersonación…).

ITEM	CONTROL DE ACCESO A LA RED (NAC)
55	* Eventos de seguridad recibidos de otras plataformas, y las acciones tomadas
56	* Resultado de los escaneos de compliance (fallados, pasados)
57	* Histórico de dispositivos conectados, última conexión…)
58	La solución debe incluir plantillas de reportes, ejecutables bajo demanda o programados).
59	La solución debe permitir customizar los reportes.
60	La solución debe de incluir plantillas de despliegue de políticas.
61	La solución debe de permitir la opción de usar un Sistema de reporte y monitorización dedicado.

3.6. SOLUCIÓN DE ACCESOS PRIVILEGIADOS (PAM)

ITEM	CONTROL DE ACCESO PRIVILEGIADO (PAM) – 30 USUARIOS
1	Se requiere solución PAM tipo appliance virtual o físico para mínimo 30 usuarios privilegiados.
2	La solución deberá permitir integración con dispositivos de seguridad perimetral (firewalls u otros) para control de acceso privilegiado mediante políticas centralizadas, ya sea de forma nativa o mediante mecanismos estándar de integración.
3	La solución deberá permitir integración con herramientas de análisis de logs para envío de registros y trazabilidad avanzada, mediante mecanismos estándar (Syslog, API, conectores o equivalentes).
4	La solución deberá integrarse con plataformas SIEM para correlación de eventos de sesiones privilegiadas.
5	La solución deberá soportar autenticación multifactor (MFA), ya sea de forma nativa o mediante integración con soluciones externas.
6	La solución debe permitir administración centralizada de cuentas privilegiadas locales y de dominio.
7	La solución deberá contar con bóveda cifrada de credenciales utilizando algoritmos de cifrado robustos reconocidos por la industria (ej. AES-256 o equivalente).
8	La solución debe soportar rotación automática de contraseñas configurable por política.
9	La solución debe permitir acceso Just-In-Time (JIT) para elevación temporal de privilegios.
10	La solución debe permitir grabación completa de sesiones (video y comandos) para auditoría.
11	La solución debe permitir monitoreo en tiempo real de sesiones activas.
12	La solución debe permitir terminación forzada de sesiones activas por parte del administrador.
13	La solución debe soportar acceso a servidores Windows vía RDP sin exponer credenciales al usuario final.
14	La solución debe soportar acceso a servidores Linux/Unix vía SSH con proxy seguro.
15	La solución debe permitir acceso a dispositivos de red (switches, firewalls) mediante proxy seguro.
16	La solución deberá permitir integración con servicios de directorio (ej. Active Directory o equivalentes), preferiblemente sin requerir agentes, o mediante mecanismos que no impacten significativamente la operación.
18	La solución debe permitir políticas basadas en roles (RBAC).
19	La solución debe permitir segmentación de accesos según grupos de AD.
20	La solución debe generar reportes de cumplimiento para auditoría (ISO 27001, NIST, etc.).
21	La solución debe registrar logs detallados de comandos ejecutados en sesiones SSH.
22	La solución debe permitir aprobación previa de accesos privilegiados (workflow).

ITEM	CONTROL DE ACCESO PRIVILEGIADO (PAM) – 30 USUARIOS
23	La solución debe soportar arquitectura de alta disponibilidad (HA).
24	La solución deberá permitir despliegue en entornos virtualizados, físicos o en la nube, incluyendo pero no limitado a VMware, Hyper-V, KVM o proveedores cloud.
25	La solución deberá permitir integración con servicios de identidad en la nube (ej. Azure AD u otros proveedores equivalentes).
26	La solución debe permitir descubrimiento automático de cuentas privilegiadas en la red.
27	La solución debe permitir gestión de cuentas de servicio.
28	La solución debe permitir control de acceso a bases de datos mediante proxy.
29	La solución debe permitir acceso seguro a aplicaciones web administrativas.
30	La solución debe permitir control granular por horario y geolocalización.
31	La solución debe permitir aplicar políticas Zero Trust para accesos administrativos.
32	La solución debe permitir segregación de funciones administrativas.
33	La solución debe permitir exportación de reportes en PDF y CSV.
34	La solución debe permitir integración con SIEM externo vía Syslog.
35	La solución debe contar con dashboard ejecutivo en GUI web.
36	La solución podrá integrarse con herramientas de análisis de amenazas o sandboxing para correlación de comportamiento asociado a sesiones privilegiadas.
37	La solución debe permitir control de acceso privilegiado a entornos OT.
38	La solución debe permitir definir políticas de expiración automática de accesos temporales.
39	La solución debe permitir trazabilidad completa para investigaciones forenses.
40	La solución debe incluir soporte y actualizaciones por mínimo un (1) año.
41	La solución debe incluir instalación, configuración e integración con la infraestructura existente.
42	La solución debe permitir escalabilidad futura sin cambio de plataforma.

3.7. SOLICIÓN NDR

ITEM	REQUERIMIENTO TÉCNICO MÍNIMO
1	La solución debe suministrarse bajo modalidad de servicio (SaaS o equivalente).
2	Debe incluir sensores virtuales y mecanismos de captura desplegables en ambientes on premise, cloud o híbridos. El licenciamiento de los sensores debe estar incluido acorde a las necesidades de la entidad.
3	Debe ser compatible con entornos virtualizados comunes (VMware, Hyper-V, KVM o equivalentes).
4	La solución no debe encontrarse en estado EOL/EOS durante la vigencia del contrato.
5	Debe incluir licenciamiento por suscripción mínimo de doce (12) meses, con capacidad de procesamiento de al menos 1 Gbps o equivalente.
6	Debe incluir soporte técnico del fabricante en modalidad 7x24.
7	Debe incluir actualizaciones periódicas de software, firmware e inteligencia de amenazas.
8	Debe permitir captura de tráfico mediante SPAN, TAP o mecanismos equivalentes.
9	Debe soportar análisis de tráfico en tiempo real.

ITEM	REQUERIMIENTO TÉCNICO MÍNIMO
10	Debe permitir análisis de tráfico cifrado mediante técnicas avanzadas.
11	Debe contar con capacidades de analítica avanzada para detección de amenazas.
12	Debe permitir detección de anomalías basadas en comportamiento.
13	Debe incluir capacidades de análisis de comportamiento de red o equivalente.
14	Debe proporcionar visibilidad de dispositivos en la red.
15	Debe proporcionar visibilidad de usuarios.
16	Debe proporcionar visibilidad de aplicaciones.
17	Debe permitir detección de amenazas avanzadas (APT o equivalentes).
18	Debe permitir detección de malware conocido y desconocido.
19	Debe permitir identificar el origen inicial de incidentes de seguridad.
20	Debe permitir análisis forense de eventos.
21	Debe permitir retención de información de eventos y/o metadatos por un periodo configurable (mínimo 180 días) o superior.
22	Debe generar alertas en tiempo real.
23	Debe permitir integración con soluciones de seguridad (ej. firewalls, SIEM, SOAR, entre otros).
24	Debe permitir capacidades de respuesta o contención ante incidentes (manual o automática).
25	Debe permitir integración mediante API o mecanismos equivalentes.
26	Debe permitir integración con herramientas de análisis o sandboxing.
27	Debe permitir exportación de logs en formatos estándar.
28	Debe permitir generación de reportes personalizados.
29	Debe incluir dashboards de monitoreo.
30	Debe permitir búsqueda avanzada de eventos.
31	Debe soportar actividades de threat hunting.
32	Debe permitir mapeo de amenazas basado en estándares reconocidos (ej. MITRE ATT&CK o equivalente).
33	Debe permitir identificar la cadena de ataque.
34	Debe permitir análisis de movimiento lateral.
35	Debe ser escalable sin requerir reemplazo total de la solución.
36	Debe permitir despliegue distribuido.
37	Debe garantizar alta disponibilidad del servicio.
38	Debe cumplir con estándares de seguridad de la industria.
39	Debe permitir clasificación y correlación de eventos.
40	Debe permitir integración con el ecosistema del fabricante u otros fabricantes.
41	Debe incluir servicios de implementación del contratista o fabricante. Adicionalmente debe incluir servicios de profesionales directamente del fabricante durante la vigencia del contrato.
42	Debe incluir documentación técnica.

ITEM	REQUERIMIENTO TÉCNICO MÍNIMO
43	Debe permitir monitoreo continuo.
44	Debe permitir análisis retrospectivo.

3.8. SOLUCIONES PARA REALIZAR PRUEBAS DINAMICAS DE SEGURIDAD DE APLICACIONES

ITEM	REQUERIMIENTO TÉCNICO MÍNIMO
Análisis dinámico de seguridad de aplicaciones	Solución de prueba de seguridad de aplicaciones que debe tener la capacidad de simular ataques reales en una aplicación en ejecución para encontrar vulnerabilidades, como mínimo que soporte un enfoque de «caja negra», y que no requiera conocer el código interno ni la estructura de la aplicación, sino que realice las pruebas desde una perspectiva externa, similar a la del usuario
	Debe tener la capacidad de detectar las principales vulnerabilidades de owasp y otras vulnerabilidades, así como generar información detallada sobre las vulnerabilidades encontradas.
	La solución debe contar con capacidad para realizar pruebas de seguridad para mínimo 120 aplicaciones
Análisis de composición de Software	La solución debe incluir licencias para seguridad de código que incluya análisis de composición de software, pruebas de seguridad de aplicaciones estáticas (sast), seguridad en infraestructura como código, secretos, cumplimiento de licencias y listado de software para mínimo 20 desarrolladores
	La solución debe identificar y analizar componentes open-source y librerías de terceros.
	La solución debe detectar vulnerabilidades conocidas (cve).
	La solución debe generar y mantener automáticamente un software bill of materials (sbom).
	La solución debe identificar riesgos de licenciamiento open-source.
	La solución debe proporcionar alertas priorizadas por criticidad.
Análisis estático de código Análisis de Secretos	La solución debe detectar vulnerabilidades en etapas tempranas del sdlc.
	La solución debe minimizar falsos positivos para las.
	La solución debe integrarse con repositorios (github, gitlab, bitbucket u otros).
	La solución debe permitir análisis automatizado en pipelines ci/cd.
	La solución debe identificar secretos expuestos en código (api keys, tokens, credenciales).
	La solución debe detectar credenciales embebidas en repositorios.
	La solución debe proporcionar visibilidad contextual de riesgo (attack path).
Gestión de cumplimiento de licencias	La solución debe identificar riesgos asociados a licencias open-source.
	La solución debe clasificar tipos de licencias.
	La solución debe permitir definición de políticas corporativas.
	La solución debe generar reportes para auditorías.
Lista de materiales para Software - SBOM	La solución debe generar sbom en tiempo real por aplicación.
	La solución debe proporcionar visibilidad completa de dependencias.
	La solución debe permitir exportación en formatos estándar.
Análisis dinámico de código	La solución debe simular ataques reales sobre aplicaciones en ejecución.
	La solución debe detectar vulnerabilidades desde perspectiva externa (black-box).

ITEM	REQUERIMIENTO TÉCNICO MÍNIMO
	La solución debe integrarse con entornos de staging o pre-producción.
Administración	La solución debe capacidad para proporcionar políticas totalmente integradas en todos los conjuntos de características.
	La solución debe capacidad para obtener una funcionalidad completa con api y cli.
	La solución debe posibilidad de exportar informes y reportes.
Informes	La solución debe posibilidad de programar y enviar informes por correo electrónico
	La solución debe posibilidad de exportar informes en pdf, csv y html.
	La solución debe posibilidad de conservar los datos por un periodo de tiempo.
	La solución debe capacidad para proporcionar informes detallados para la utilización y licenciamiento
Integraciones	La solución debe capacidad para buscar vulnerabilidades en el pipeline de ci a través de la integración con herramientas de desarrollo como jenkins
	La solución debe capacidad para admitir la sincronización bidireccional que permite compartir y actualizar alertas entre herramientas de flujo de trabajo como jira
	La solución debe capacidad de integración con herramientas siem/soar como splunk, fortisiem, qradar
	Despliegue en nube

4. CARACTERÍSTICAS GENERALES

El oferente debe cumplir los siguientes requisitos:

a. El oferente deberá aportar certificación dada por el fabricante que lo acredite en la categoría de el nivel más alto en Colombia, por ejemplo, en nivel Gold, Signature, Expert o Platinum, según la equivalencia en cada fabricante; para lo cual deberá entregar una certificación expedida por el fabricante con vigencia no menor de 30 días con el número del proceso.
b. Adicional a la membresía de Partner, el oferente deberá contar con las especializaciones vigentes que lo acrediten en los productos ofertados, con el fin de garantizar que dispone de personal certificado y con las competencias técnicas necesarias para la adecuada prestación del servicio.
c. El oferente debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, entre otros) requerida para que el personal asignado al proyecto pueda cumplir sus funciones.
d. Se debe realizar la puesta en funcionamiento del licenciamiento y dispositivos adquiridos, así como la integración con las plataformas de seguridad con las que cuenta la Secretaría Distrital de Salud.
e. Todas las implementaciones deben ser realizadas por un ingeniero certificado a nivel profesional y especialista por el fabricante.
f. El licenciamiento requerido debe tener soporte en un esquema 7 x 24 ante fabricante que incluya actualizaciones de firmware.

g. *El oferente deberá hacer dos ejercicios de RED TEAM a toda la infraestructura tecnológica* ***de la entidad*** *durante* ***el periodo de soporte y garantía contratado***.
h. Garantizar soporte y garantía a los equipos de seguridad perimetral adquiridos, durante el periodo de la garantía.
i. Se debe realizar una transferencia de conocimiento de un total de 20 horas, donde se vean temas de administración de resolución de problemas de las plataformas de seguridad adquiridas, a mínimo tres (3) personas designadas por el supervisor del contrato.
j. Crear reportes cuando se aplique soporte y garantía de acuerdo con las solicitudes realizadas por el supervisor del contrato para las plataformas y licencias adquiridas.
k. El oferente deberá contar con certificación vigente ISO/IEC 20000, la cual garantice que dispone de un Sistema de Gestión de Servicios de TI (SGSTI) implementado y auditado, asegurando la adecuada gestión, control y mejora continua de sus procesos y servicios tecnológicos.
l. El oferente deberá contar con certificación vigente ISO/IEC 27001, la cual garantice que dispone de un Sistema de Gestión de Seguridad de la Información (SGSI) implementado y auditado, asegurando el adecuado manejo, protección y control de la información, así como la gestión segura de sus procesos y servicios.

5. REQUERIMIENTOS TÉCNICOS DE INSTALACIÓN

- El oferente debe realizar la planeación de cada una de las actividades, validadas en conjunto con la Secretaría Distrital de Salud y de acuerdo con la disponibilidad de la entidad.
- El oferente debe realizar la configuración y alistamiento del software y firmware del hardware a la última versión estable aprobada por el fabricante para todas las plataformas licenciadas.
- El oferente deberá entregar las licencias y dispositivos adquiridos en el sitio indicado por la Secretaría Distrital de Salud.
- El oferente deberá realizar la configuración y activación de las licencias en cada una de las plataformas, así como el respectivo registro en la página web del fabricante.
- El oferente deberá entregar toda la documentación requerida de la instalación y configuración de las licencias y productos con sus topologías de red.

6. TRANSFERENCIA DE CONOCIMIENTO

El contratista deberá realizar transferencia de conocimiento durante mínimo ocho (8) horas por solución, a tres (3) ingenieros del Grupo de TIC, designados por el Supervisor del contrato, orientada a la instalación, configuración, parametrización y puesta en marcha de la solución, que brinde el conocimiento necesario para la administración y operación del hardware y software de la solución de seguridad implementada.
La transferencia de conocimiento se podrá realizar durante la instalación, configuración, parametrización y puesta en funcionamiento la solución.
Previo al inicio de actividades, el contratista deberá hacer entrega del documento de Plan de Transferencia de conocimiento en el cual se debe describir el mecanismo a utilizar para dicha

actividad, de tal manera que se logre efectuar un aprovechamiento óptimo del software, de los equipos y de la tecnología.

7. SERVICIOS PROFESIONALES

La solución deberá incluir los servicios de diseño, instalación, configuración, parametrización, puesta en funcionamiento y entrega a satisfacción, realizada por ingenieros certificados por el fabricante de los equipos. El contratista deberá presentar las respetivas certificaciones del grupo de trabajo asignado expedidas por el fabricante de los equipos.
El contratista deberá presentar máximo tres (3) días hábiles luego de firmada el acta de inicio las hojas de vida y certificaciones del personal que realizará la implementación y el plan de trabajo detallado en el cual se describa el componente de diseño de la seguridad perimetral

incluyendo los equipos que actualmente cuenta la entidad, adicionalmente se debe tener en cuenta los procesos/actividades inherentes para alcanzar el objeto de la solución, explicando claramente el número de días de la actividad y profesionales dedicados para desarrollar cada actividad relacionada en el cronograma, que incluya, entre otros, actividades, fechas de inicio y terminación, hitos y ruta crítica. La secuencia y duración de cada una de las actividades debe estar discriminada en semanas. Este plan de trabajo será de obligatorio cumplimiento durante la ejecución del contrato, previa aprobación del Supervisor del Contrato
Los diseños de la solución a implementar deberán ser revisados y aprobados por el supervisor del contrato. Si el Supervisor lo considera pertinente podrá solicitar nuevos diseños que se ajusten a las necesidades de la Entidad.
Planeación de cada una de las actividades con el fin de disminuir los tiempos de afectación en el servicio.
Presentar diseño de seguridad perimetral de acuerdo con buenas prácticas y recomendaciones del fabricante integrando los dispositivos de seguridad con los que actualmente cuenta la entidad, este será evaluado y aprobado por el supervisor de contrato.
Presentar el diseño de Políticas de Seguridad para ser evaluado y aprobado por el líder de infraestructura y el supervisor del contrato.
Configuración y alistamiento del software, hardware y firmware a la última versión estable aprobada por el fabricante.
Implementación de la solución de acuerdo con las mejores prácticas de los fabricantes, teniendo en cuenta una arquitectura de red segura.
Pruebas de Servicio de las plataformas ofertadas.
Puesta en Producción de las plataformas ofertadas.
Estabilización de las plataformas ofertadas.
Entrega a satisfacción de la entidad.
Dentro de los servicios se debe tener en cuenta el diseño, Instalación, configuración y puesta en producción de los dispositivos de seguridad que actualmente cuenta la Entidad, así como la entrega a satisfacción de los mismos a la entidad, realizando todas las tareas necesarias para cumplir con ello, sin que esto genere gastos o cobros adicionales para el cliente.
La entidad requiere la implementación y puesta en marcha de las plataformas ofertadas, así como la configuración de políticas, objetos y demás configuraciones a que haya lugar para dejar las misma totalmente operativas y a satisfacción de la entidad, así como realizar pruebas de

detección de cada una para validar su correcta configuración de acuerdo con las buenas prácticas de implementación del fabricante.
El oferente debe contemplar en su oferta todos los costos o gastos asociados a la logística (desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, Entre otros) requerida para que el personal asignado al proyecto pueda cumplir sus funciones.

8. DOCUMENTACIÓN

El contratista debe adjuntar los folletos, catálogos u hojas de especificaciones técnicas de los productos y servicios ofrecidos.

El contratista debe documentar todos los procedimientos realizados para la instalación, configuración y parametrización de cada una de las funcionalidades implementadas y entregarlos en medio magnético e impreso, una vez revisados y aprobados por el Supervisor del contrato.

Al finalizar la puesta en funcionamiento de la solución contratada, debe entregar en medio magnético o impreso, la documentación que permita la eficiente administración, como mínimo incluir: * Manual de procedimientos de administración y operación de los appliances. Documento de descripción de la configuración de appliance y parámetros de configuración inicial de todo el software instalado. * Documentación de la topología de la solución implementada.

9. REQUERIMIENTOS TÉCNICOS EN FUNCIONAMIENTO

El contratista deberá realizar y documentar entre otras, las siguientes actividades previa coordinación con el supervisor del contrato en desarrollo:

a. Revisar y configurar las licencias ofertadas en todas las plataformas.
b. Configurar, afinar y revisar los reportes / logs de las plataformas.
c. Implementar la solución de acuerdo con las mejores prácticas del fabricante, teniendo en cuenta una arquitectura de red segura.
d. Poner en producción las plataformas, realizando la integración con las demás plataformas de seguridad de la Secretaría Distrital de Salud.
e. Poner en producción las licencias ofertadas, realizando la integración con las demás plataformas de seguridad de la Secretaría Distrital de Salud.
f. Ejecutar pruebas de servicio de las plataformas licenciadas donde se evidencie la correcta configuración y afinamiento de cada plataforma licenciada y los servicios de la entidad asociados.
g. Mantener actualizado el firmware de los componentes ofertados, de acuerdo con las últimas versiones estables liberadas por el fabricante con aprobación de la Secretaría Distrital de Salud.
h. Posterior a la instalación y puesta en marcha, realizar el afinamiento y estabilización de las plataformas adquiridas y licenciadas.
i. Entregar las soluciones a satisfacción de la Secretaría Distrital de Salud.

10. INDICADORES Y ANS MESA DE AYUDA

Este documento establece las condiciones generales de los servicios que el contratista deberá prestar en virtud del contrato, conforme a las disposiciones legales aplicables en materia de contratación estatal. Así mismo, detalla los tiempos de respuesta que deben ser cumplidos en función de la clasificación de los incidentes y las solicitudes, los cuales se regirán por los principios de transparencia, eficiencia y buena fe, que rigen el marco normativo de la contratación pública. En caso de vacíos o situaciones no contempladas en este documento, se deberán aplicar las normas ITIL como estándar de buenas prácticas para la gestión de servicios tecnológicos.

11. CONDICIONES DEL SOPORTE

El contratista deberá disponer de diferentes medios de comunicación para atender y resolver todas las asesorías técnicas necesarias para una adecuada instalación, configuración, operación, soporte y diagnóstico de los equipos y/o elementos que componen la solución de seguridad perimetral.

El tiempo de solución depende en gran medida de la interacción entre el contratista y la Secretaría Distrital de Salud. El contratista se compromete a tener los medios necesarios para escalar los casos directamente a fábrica sin costo adicional para la Secretaría Distrital de Salud.

El tiempo de solución, para todos los niveles, se detendrá cuando se estén realizando actividades cuya responsabilidad sea de la Secretaría Distrital de Salud.

Cuando el personal designado por de la Secretaría Distrital de Salud reporte una falla es importante tener en cuenta la siguiente información:

- Tipo de problema. (Aleatorio, frecuente, falla total, falla parcial).
- Descripción del problema, frecuencia, situación, lugar físico del problema.
- Información técnica (Diagramas de red LAN, WAN o de servicios).
- Descartar fallas externas.
- Tener claro conocimiento del problema.
- Status del sistema (errores, debugs, logs de eventos).

El contratista, se compromete a proporcionar un número telefónico y un e-mail disponible durante el tiempo de garantía de la solución para brindar atención de llamadas 5X8 de consultas técnicas, reportes de fallas y seguimiento de estas.

Se brindará un diagnóstico remoto de la causa del incidente y la validación de la posibilidad de la solución vía remota. También se le indicará a la persona designada por de la Secretaría Distrital de Salud, las posibles acciones requeridas. Luego de alcanzar la solución al inconveniente reportado esta se corroborará mediante un chequeo de funcionamiento, y luego de esto el cliente debe autorizar el cierre del caso.

El oferente deberá contar con las certificaciones Engage Preferred Services Partner y Engage Tech Support Partner, otorgadas por el fabricante, con el fin de garantizar que dispone del respaldo directo del fabricante para la prestación de servicios profesionales, soporte técnico especializado e implementación de las soluciones objeto del presente proceso.

Soporte técnico vía web

El contratista, deberá contar con un software para el manejo de Tickets a través de su página WEB.

Por medio de este sistema el personal de la Secretaría Distrital de Salud que se designe será autorizado por el contratista para tener acceso y control sobre sus tickets abiertos y cerrados, permitiéndoles realizar consultas que puedan servir de ayuda para la solución de un caso actual.

Soporte vía email

El contratista, se compromete a proporcionar un e-mail de contacto a través del cual personal autorizado por de la Secretaría Distrital de Salud podrá requerir los servicios de atención de fallas, consultas sobre el estado de los ticket e información relacionada con el objeto de estos Términos de invitación.

La supervisión designará el personal que estará autorizado para gestionar asuntos relacionados con el presente contrato y recibir los informes que se generen del mismo, indicando los datos de contacto a los que se reportarán los soportes establecidos por los mecanismos descritos, su avance y su cierre.

Soporte telefónico

El contratista, se compromete a proporcionar un número telefónico y un e-mail disponible durante el tiempo acordado para brindar atención de llamadas 5x8 de consultas técnicas, reportes de fallas y seguimiento de estas.

El Soporte Técnico Telefónico no tiene un límite de llamadas.

Soporte remoto

El contratista deberá brindar diagnóstico remoto de la causa del incidente y la validación de la posibilidad de la solución vía remota. También le indicará a la persona designada por de la Secretaría Distrital de Salud, las posibles acciones requeridas. Luego de alcanzar la solución al inconveniente reportado esta se corroborará mediante un chequeo de funcionamiento, y luego de esto de la Secretaría Distrital de Salud debe autorizar el cierre del caso.

Soporte técnico en sitio

El contratista deberá ofrecer el servicio de soporte técnico en sitio con el personal idóneo para realizar la instalación, operación y resolución de fallas.

Este soporte se activa por el servicio de soporte remoto o por la falta de este, en caso de que sea imposible realizarlo. En este, se dará el diagnóstico de la probable causa del incidente y el plan (repuestos) al área encargada por el contratista.

Durante el ciclo de vida de la incidencia se cumplen completamente con los Acuerdos de Niveles de Servicio SLA acordados y descritos en el siguiente capítulo.

12. ACUERDO DE NIVELES DE SERVICIO DEL LOS EQUIPOS ADQUIRIDOS

El tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio y plan de comunicaciones se describen a continuación.

NIVEL DE TIPO DE FALLA SEVERIDAD	NIVEL DE TIPO DE FALLA SEVERIDAD	DESCRIPCIÓN
FALLA CRITICA	S1	Los equipos dejaron de funcionar por completo, ocasionando un impacto critico en las operaciones de la solución de seguridad de la Secretaría Distrital de Salud.
FALLA GRAVE	S2	Los equipos han dejado de funcionar parcialmente, ocasionando un impacto medio en las operaciones de la solución de seguridad de la Secretaría Distrital de Salud. Algunas operaciones continúan funcionando normalmente.
FALLA LEVE	S3	El sistema no funciona de manera óptima, aunque muchas de las operaciones continúan funcionando correctamente, el impacto es bajo en la solución de seguridad de la Secretaría Distrital de Salud
REQUERIMIENTOS DE SERVICIO	S4	El usuario final requiere información o asistencia sobre las posibilidades, la instalación o configuración de nuevos requerimientos. Se tratan también los problemas comunes con muy bajo impacto en la solución de seguridad de la Secretaría Distrital de Salud

Tiempos de respuesta

El registro de cualquier incidencia se puede realizar en cualquier momento del día a cualquier hora por los medios dispuestos para ello por el contratista, sin embargo, solo se tendrá en cuenta en el horario de atención establecido en el contrato.
Los tiempos de respuesta de acuerdo con la clasificación del incidente registrado son los siguientes:

TIEMPO DE RESPUESTA		
NIVEL DE SEVERIDAD	**TELEFONICO/REMOTO TIEMPO DE RESPUESTA EN SITIO PARA DIAGNÓSTICO**	**TIEMPO DE RESPUESTA EN SITIO**
S1	30 MINUTOS	Ingeniero en sitio antes de 4 horas, contado a partir del reporte de la falla, atención 7*24*365
S2	MENOS DE 60 MINUTOS	Ingeniero en sitio antes de 6 horas, contado a partir del reporte de la falla, atención 7*24*365

TIEMPO DE RESPUESTA		
NIVEL DE SEVERIDAD	**TELEFONICO/REMOTO TIEMPO DE RESPUESTA EN SITIO PARA DIAGNÓSTICO**	**TIEMPO DE RESPUESTA EN SITIO**
S3	MENOS DE CUATRO HORAS	Visita programada dentro de las siguientes ocho (8) horas hábiles, contado a partir del reporte de la falla para el siguiente horario: L-V de 7:00am a 5:00 pm S de 7:00 am a 1:00pm
S4	SIGUIENTES OCHO	Visita programada dentro de las siguientes veinticuatro (24) horas hábiles, contado a partir del reporte de la falla para el siguiente horario: L-V de
	HORAS HABILES	7:00am a 5:00 pm
	ANTES DE 24 HORAS HABILES	S de 7:00 am a 1:00pm

Nota: El plazo de ejecución del contrato está definido en los estudios previos.

El contratista se compromete a aplicar garantías, y dar solución a incidentes y requerimientos en un lapso no mayor a 48 horas. En caso de ser necesario el retiro o suspensión de algún componente por más de 48 horas, el contratista debe suministrar inmediatamente un componente que garantice el servicio de conectividad de manera temporal mientras se restituye o reemplaza el componente afectado.

Los componentes entregados en reemplazo (temporal o definitivo) deben cumplir con las mismas o mejores características ofertadas.

13. EQUIPO DE TRABAJO

Las hojas de vida del personal de trabajo no son requisito habilitante y deben ser entregadas por el contratista después de la adjudicación del presente proceso.

GERENTE DE PROYECTO

Gerente de proyecto dedicación 100%, Profesionales Ingeniero de Sistemas, Electrónico o de Telecomunicaciones, con tarjeta vigente.

Pregrado: Ingeniera de Sistemas, ingeniería en telemática y afines o Ingeniería Electrónica, ingeniería en telecomunicaciones y afines
Posgrado: máster y/o especialización en gerencia de proyectos de tecnologías de la información
Experiencia: mínimo nueve (9) años de experiencia general a partir de la t.p. Y (5) años de experiencia especifica en proyectos de tecnología como gerente o director de proyectos, esta será acredita mediante certificaciones de experiencia laboral.
Certificaciones requeridas: el profesional postulado debe contar con tes (3) de las certificaciones que se relacionan a continuación:
Itil v4 foundation

Scrum foundation
Iso/iec 27001:2022 auditor interno
Pmp –project management professional

PROFESIONAL DE IMPLEMENTACION

Pregrado: Ingeniera de Sistemas, ingeniería en telemática y afines o Ingeniería Electrónica, ingeniería en telecomunicaciones y afines
Posgrado: Máster y/o especialización en seguridad informática o afines
Mínimo cinco (5) años de experiencia general a partir de la t.p. Y (3) años de experiencia especifica en proyectos de seguridad informática, esta será acredita mediante certificaciones de experiencia laboral.
Certificaciones requeridas: el profesional postulado debe contar con todas de las certificaciones que se relacionan a continuación:
Certified professional security operations
Certified solution specialist security operations
Certified professional network security
Certified solution specialist network security

PROFESIONAL DE APOYO DE SEGURIDAD INFORMATICA

Pregrado: Ingeniera de Sistemas, ingeniería en telemática y afines o Ingeniería Electrónica, ingeniería en telecomunicaciones y afines
Posgrado: Máster y/o especialización en seguridad informática o afines
Mínimo nueve (9) años de experiencia general todas contadas a partir de la expedición de la t.p., y mínimo tres (6) años de experiencia especifica en proyectos de seguridad informática, mediante la presentación de certificaciones laborales y/o contratos.
Certificaciones requeridas: el profesional postulado debe contar con cuatro (4) de las certificaciones que se relacionan a continuación:
Ceh (certified ethical hacker)
Cciso (associate certified chief information secutity officer)
Cisa (certified information systems auditor)
Cnda (certified network defense architect)

Elaborado por: Arnol Julian Martinez- Contratista TIC

Firmado digitalmente por Arnol Julian Martinez Paredes

Glosario de términos de Seguridad Informática

1. **Firewall:** Dispositivo o software que controla y filtra el tráfico de red entrante y saliente según reglas de seguridad definidas.
2. **Software:** Conjunto de programas, aplicaciones y sistemas operativos que permiten el funcionamiento de equipos informáticos.
3. **Hardware:** Componentes físicos de un sistema informático, como servidores, computadores, routers y dispositivos de almacenamiento.
4. **Suscripción:** Modalidad de licenciamiento mediante la cual se obtiene acceso a un producto o servicio por un período determinado.
5. **Licenciamiento:** Derecho de uso legal de software o herramientas tecnológicas bajo condiciones definidas por el fabricante.
6. **Antivirus:** Solución de seguridad diseñada para detectar, prevenir y eliminar software malicioso.
7. **Endpoint:** Dispositivo conectado a una red, como computadores, servidores, teléfonos móviles o tablets.
8. **VPN (Virtual Private Network):** Tecnología que permite establecer conexiones seguras y cifradas a través de Internet.
9. **SIEM (Security Information and Event Management):** Plataforma que recopila, correlaciona y analiza eventos de seguridad para detectar amenazas.
10. **IDS/IPS:** Sistemas de detección (IDS) y prevención (IPS) de intrusiones que monitorean el tráfico de red para identificar actividades maliciosas.
11. **Vulnerabilidad:** Debilidad en un sistema, aplicación o red que puede ser explotada por una amenaza.
12. **Amenaza Cibernética:** Evento o actor con capacidad de comprometer la confidencialidad, integridad o disponibilidad de la información.
13. **Gestión de Identidades y Accesos (IAM):** Conjunto de procesos y tecnologías para administrar usuarios y permisos de acceso.
14. **Autenticación Multifactor (MFA):** Método de validación de identidad que requiere dos o más factores de autenticación.
15. **Cifrado:** Técnica que transforma información en un formato ilegible para protegerla contra accesos no autorizados.
16. **Hacking Ético:** Evaluación autorizada de sistemas mediante técnicas de ataque controladas para identificar vulnerabilidades.
17. **Prueba de Penetración (Pentest):** Simulación de ataques reales para evaluar la seguridad de una infraestructura tecnológica.
18. **SOC (Security Operations Center):** Centro especializado encargado de monitorear, detectar y responder incidentes de seguridad.
19. **Gestión de Incidentes:** Proceso para identificar, analizar, contener y resolver eventos de seguridad informática.
20. **Seguridad Perimetral:** Conjunto de controles destinados a proteger la frontera entre una red interna y redes externas como Internet.