

 ICANH	PROCEDIMIENTO GESTIÓN PRECONTRACTUAL	CÓDIGO:	GC-PR-08-FO-10
		VERSIÓN:	01
	FORMATO FICHA TÉCNICA DE CONDICIONES ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN	FECHA:	10-01-2024

ANEXO 1. FICHA TÉCNICA

Adquirir la renovación de las licencias del equipo de seguridad perimetral y antivirus y renovación de las licencias de los dispositivos Access Point, y certificado SSL para el Instituto Colombiano de Antropología e Historia.

MAYO – 2026

 ICANH	PROCEDIMIENTO GESTIÓN PRECONTRACTUAL	CÓDIGO:	GC-PR-08-FO-10
		VERSIÓN:	01
	FORMATO FICHA TÉCNICA DE CONDICIONES ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN	FECHA:	10-01-2024

1. GLOSARIO

A continuación, el glosario de términos utilizados a lo largo de la ficha técnica:

ÍTEM	DESCRIPCIÓN
<i>Conexión inalámbrica</i>	<i>Tipo de conexión entre dispositivos que se lleva a cabo mediante diversas ondas del espectro electromagnético.</i>
<i>Licencia</i>	<i>Es un permiso de utilización de una tecnología para su explotación comercial. Puede tratarse de tecnologías previamente protegidas por un registro legal (patentes, derecho de autor, software) o un conocimiento desarrollado por los/las investigadores/as.</i>
<i>Firewall</i>	<i>Dispositivo de seguridad de la red que monitorea el tráfico de red —entrante y saliente— permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad establecidas.</i>
<i>Antivirus</i>	<i>Software que brinda protección a los dispositivos de los usuarios contra diferentes tipos de amenazas virtuales. Así, analiza los archivos almacenados en los equipos, detecta y elimina el malware (software malintencionado).</i>
<i>Seguridad</i>	<i>Seguridad es la capacidad de dar respuesta efectiva a riesgos, amenazas o vulnerabilidades y estar preparados para prevenirlos, contenerlos y enfrentarlos.</i>
<i>Malware</i>	<i>Cualquier tipo de software malicioso diseñado para dañar o explotar cualquier dispositivo, servicio o red programable.</i>
<i>Phishing</i>	<i>Es un ataque que intenta robar el dinero o identidad, haciendo que divulgue información personal (como números de tarjeta de crédito, información bancaria o contraseñas) en sitios web que fingen ser sitios legítimos.</i>
<i>Vulnerabilidad</i>	<i>Una vulnerabilidad de seguridad es cualquier fallo o debilidad en la estructura, funcionalidad o implementación de una red o activo en red que los hackers pueden explotar para lanzar ciberataques, obtener acceso no autorizado a sistemas o datos o dañar a una organización</i>
<i>VPN</i>	<i>VPN (Red Privada Virtual) es una tecnología que crea una conexión segura y cifrada entre el dispositivo (como un computador, teléfono o tableta) e Internet. Esta conexión actúa como un “túnel” que protege la información personal, incluso si se está usando una red pública.</i>
<i>Certificado SSL</i>	<i>Archivo digital que autentica la identidad de un sitio web y cifra la conexión entre el navegador del usuario y el servidor web</i>

 ICANH	PROCEDIMIENTO GESTIÓN PRECONTRACTUAL	CÓDIGO:	GC-PR-08-FO-10
		VERSIÓN:	01
	FORMATO FICHA TÉCNICA DE CONDICIONES ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN	FECHA:	10-01-2024

2. INTRODUCCIÓN

El Instituto Colombiano de Antropología e Historia es una entidad pública del orden nacional perteneciente al sector cultura. Máxima autoridad en materia de patrimonio arqueológico de la nación; realiza y promueve la investigación y la divulgación de conocimientos sobre la diversidad étnica y cultural, con comunidades y grupos involucrados desde una perspectiva temporal amplia. Es un órgano asesor de la gestión y la política pública.

Que el Instituto Colombiano de Antropología e Historia, tiene como misión institucional investigar, generar, difundir y transferir conocimientos antropológicos, arqueológicos, históricos y del patrimonio cultural. Así mismo, aporta elementos críticos y propositivos relativos a la diversidad cultural colombiana, para orientar y gestionar políticas estatales tendientes a la protección del patrimonio y promover el diálogo intercultural.

Para el año 2032 el Instituto Colombiano de Antropología e Historia se proyecta como una entidad con presencia regional fortalecida que encara los desafíos globales, reconoce las diferencias sociales, y facilita el diálogo y la gobernanza intercultural. Es referente en la producción y democratización del conocimiento; y orientador en la gestión integral del patrimonio arqueológico de la nación como un principio ordenador del territorio con enfoque sostenible.

El ICANH tiene como objetivos estratégicos, los siguientes: “1. Patrimonio arqueológico y ordenamiento territorial: Fortalecer la gestión del patrimonio arqueológico como determinante en el ordenamiento territorial que integra múltiples dimensiones de la vida social, económica, política, ambiental y cultural para la construcción sostenible y democrática de los territorios. 2. Vidas campesinas, prácticas socio-espaciales y vida común: Comprender las prácticas y dinámicas sociales de las vidas campesinas y de las relaciones urbano-rurales, su especificidad socio-espacial y cultural, para la toma de decisiones en la política pública con énfasis en territorio, hábitat, alimentos, energía y agua. 3. Diferenciación social y lucha contra la discriminación: Avanzar en la comprensión de las relaciones y dinámicas sociales que generan procesos de diferenciación y jerarquización social con el fin de incidir en políticas y gestión pública incluyentes que superen diferentes formas de discriminación. 4. Presencia regional y fortalecimiento de las capacidades institucionales para el cambio: Fortalecer las capacidades organizacionales e institucionales en investigación, divulgación, fomento, infraestructura, articulación interinstitucional, gestión pública y administrativa para robustecer la presencia regional, disminuir brechas de desigualdad social y garantizar derechos. 5. Conocimiento público para la construcción de la paz: Fortalecer los procesos de producción, coproducción, fomento y divulgación del conocimiento y la investigación interdisciplinaria en la esfera pública con un enfoque de construcción de la paz. 6. Apropiación e innovación social para la gobernanza intercultural: Promover la participación de la ciudadanía y las organizaciones sociales en los procesos misionales con el fin de generar apropiación e innovación social, y aportar a la gobernanza intercultural”.

Así mismo, el artículo 4 del Decreto 0993 del 17 de septiembre de 2025, establece como funciones generales del ICANH, entre otras, las siguientes: “(...) 2. Asesorar y orientar a las entidades del orden nacional, regional y local, en el diseño e implementación de planes y proyectos concernientes a la diversidad étnica y cultural del país, representada en comunidades indígenas, negras, afrocolombianas, raizales y palenqueras, rom, etc., a partir del conocimiento de los campos de la antropología, la arqueología y la historia, de acuerdo con las normas vigentes. (...) 4. Implementar los mecanismos necesarios para la efectiva presencia institucional en las regiones

 ICANH	PROCEDIMIENTO GESTIÓN PRECONTRACTUAL	CÓDIGO:	GC-PR-08-FO-10
		VERSIÓN:	01
	FORMATO FICHA TÉCNICA DE CONDICIONES ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN	FECHA:	10-01-2024

del país, en actividades de investigación, divulgación y apropiación social en los campos misionales del Instituto. (...) 11. Diseñar, formular, implementar y hacer seguimiento a las acciones estratégicas que promuevan la valoración, la democratización y la apropiación social en los campos misionales del ICANH, así como del conocimiento sobre la diversidad cultural y étnica del país, a partir de un enfoque participativo (...).

Que por su parte, el Artículo 10 del Decreto 0993 de 2025, establece algunas normas en las Funciones de la Dirección General, las cuales están orientadas a soportar la plataforma tecnológica: “(...). 2. Orientar la investigación y publicación de conocimientos en los campos de antropología, arqueología e historia, así como los demás componentes afines o relacionados con las competencias del Instituto (...). (...) 9. Orientar las políticas institucionales en materia de gestión tecnológica requeridas para el cumplimiento del objeto del ICANH”

Que en el mismo sentido, el Decreto 0993 del 17 de septiembre de 2025, establece en el Artículo 15 las funciones de la Oficina de Tecnologías, de la siguiente manera: “1. Definir los lineamientos y estándares para el ICANH sobre el gobierno de tecnologías de la información y las comunicaciones (TIC), de conformidad con la normativa vigente. 2. Definir, aplicar y controlar los lineamientos institucionales que orientan la gestión tecnológica del ICANH, para contribuir al logro de los objetivos estratégicos de la entidad. 3. Liderar y coordinar con las demás áreas del ICANH, la implementación del Plan de Gobierno y Gestión de la Información, así como la aplicación de políticas y estándares para garantizar el acceso y uso de la información institucional. 4. Implementar los lineamientos de política y estándares relacionados con el diseño y desarrollo de proyectos de infraestructura tecnológica y servicios de TIC, la interoperabilidad de sistemas de información, el marco de referencia de arquitectura empresarial, el modelo de seguridad y privacidad de la información y la prestación de los servicios ciudadanos digitales, de acuerdo con la misionalidad del ICANH. 5. Administrar técnicamente los bienes y servicios tecnológicos del ICANH y brindar el soporte técnico requerido para asegurar el cumplimiento de los objetivos y funciones de la entidad. 6. Garantizar el óptimo funcionamiento de la plataforma tecnológica del ICANH, así como proponer soluciones de TIC, siguiendo las políticas y los parámetros de operación y evaluación definidos por el Instituto, de acuerdo con los lineamientos del Modelo de Gobierno de Tecnologías de la Información. 7. Definir, implementar, ejecutar, hacer seguimiento y divulgación del Plan Estratégico de Tecnologías y de la Información (PETI), de acuerdo con los lineamientos establecidos por el Gobierno Nacional. 8. Planear, ejecutar y coordinar acciones encaminadas a la articulación y promoción del desarrollo de capacidades de los servidores del ICANH en materia de uso y apropiación de TIC. 9. Definir, adoptar y aplicar lineamientos y políticas relacionadas con la adquisición, instalación, actualización y/o funcionamiento de los sistemas de información e infraestructura tecnológica del ICANH, de acuerdo con los lineamientos del Modelo de Gobierno de Tecnologías de la Información. 10. Identificar oportunidades para adoptar nuevas tendencias tecnológicas que generen impacto en el desarrollo misional del Instituto. 11. Suministrar información para la rendición de cuentas, atender a los requerimientos y solicitudes de los organismos de control internos y externos, de acuerdo con lo establecido en la normatividad vigente. 12. Liderar y participar en las políticas del Modelo Integrado de Planeación y Gestión (MIPG) que le sean asignadas. 13. Las demás funciones que le sean asignadas y que correspondan a la naturaleza de la dependencia, conforme a la normativa vigente”.

En cumplimiento de su misión institucional y en atención al plan de contratación previsto para la actual vigencia, se programó el desarrollo del proyecto que tiene como meta “Administrar y soportar la infraestructura tecnológica del Instituto Colombiano de Antropología e Historia (ICANH), incluyendo la plataforma de seguridad, redes y comunicaciones”.

 ICANH	PROCEDIMIENTO GESTIÓN PRECONTRACTUAL	CÓDIGO:	GC-PR-08-FO-10
		VERSIÓN:	01
	FORMATO FICHA TÉCNICA DE CONDICIONES ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN	FECHA:	10-01-2024

En este sentido, para el Instituto Colombiano de Antropología e Historia - ICANH es fundamental garantizar el funcionamiento óptimo de su plataforma tecnológica. En cumplimiento de las funciones asignadas a la Oficina de Tecnologías, se hace necesaria la contratación de diversos servicios tecnológicos que permitan soportar tanto la operación interna como los procesos misionales, estratégicos y de divulgación de la entidad.

Acorde con las funciones propias de la Oficina de Tecnologías, a continuación, se relacionan los servicios tecnológicos que requieren la renovación de licencias:

1) Seguridad perimetral, antivirus y gestión de vulnerabilidades

En la actualidad, para las entidades es indispensable contar con un sistema de seguridad que permita monitorear y dar soporte a cualquier eventualidad sobre la infraestructura tecnológica referente a ataques de red, software malicioso, robo o secuestro de información, mal uso de las herramientas informáticas. Estas medidas se encuentran alineadas con los principios de disponibilidad, integridad y confidencialidad previstos en buenas prácticas internacionales de seguridad de la información, como la norma ISO/IEC 27001:2022. “Sistema de Gestión de Seguridad de la Información” que proporciona un marco de trabajo con el objetivo de asegurar lo siguiente:

- Disponibilidad: La información debe estar disponible cuando se necesite.
- Integridad: Se debe proteger que la información no se modifique sin autorización.
- Confidencialidad: La información debe estar protegida de accesos no autorizados.

Actualmente, el ICANH cuenta en su centro de datos principal con una infraestructura de seguridad perimetral en alta disponibilidad Activo-Pasivo, compuesta por dos equipos con capacidades de procesamiento equivalentes a la referencia XGS4300, los cuales forman parte de la plataforma tecnológica adquirida mediante los contratos de prestación de servicios 207-2022 y 525-2024.

La solución requerida deberá garantizar plena compatibilidad técnica e interoperabilidad con la infraestructura de seguridad perimetral actual de la entidad (dispositivo referencia XGS4300), asegurando su integración nativa, continuidad operativa y la no afectación de los servicios institucionales. Para ello, se requiere la suscripción de licenciamiento que habilite las funcionalidades de firewalling, administración centralizada y orquestación de políticas bajo esquemas de seguridad sincronizada. Esta condición garantiza el pleno funcionamiento de los dispositivos y permiten entre otras funcionalidades la administración centralizada del sistema, la protección frente a correos electrónicos maliciosos, el filtrado de políticas de seguridad para las redes interna y externa, así como la conexión mediante VPN para el acceso remoto controlado a la red institucional. Así mismo, la interoperabilidad con la solución de protección endpoint actualmente desplegada en la entidad permite una gestión de seguridad integrada y sincronizada. Esta capacidad técnica garantiza altos niveles de visibilidad y una respuesta automatizada y coordinada ante amenazas como ciberataques, malware y phishing, mitigando de manera proactiva los riesgos críticos para la infraestructura tecnológica.

Descrito lo anterior, la entidad cuenta con una solución antivirus endpoint que se encuentra integrado con la solución perimetral firewall, facilitando la administración de los dos servicios a través de una consola unificada (Plataforma de administración y monitoreo en tiempo real); el antivirus permite realizar análisis de vulnerabilidades a las estaciones de trabajo y a los dispositivos que se conectan vía USB, controla la

 ICANH	PROCEDIMIENTO GESTIÓN PRECONTRACTUAL	CÓDIGO:	GC-PR-08-FO-10
		VERSIÓN:	01
	FORMATO FICHA TÉCNICA DE CONDICIONES ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN	FECHA:	10-01-2024

descarga de archivos y aplicaciones desde internet, y permite realizar bloqueos a nivel de usuarios para ejecutar cualquier aplicación o navegación en páginas web.

Por las consideraciones anteriormente expuestas, la renovación del licenciamiento para la solución de firewall y antivirus, proporciona protección contra programas maliciosos, cortafuegos de cliente, escaneado de DLP con control de contenido y gestión de dispositivos de almacenamiento extraíbles, software no autorizado, ofreciendo la mejor protección preventiva y funciones de supervisión y control de las estaciones de trabajo, los usuarios y ordenadores con plataformas basadas en Windows, Mac, Linux, UNIX y otras plataformas. Esto le proporcionará al Instituto Colombiano de Antropología e Historia – ICANH, lo siguiente:

- **Protección rápida y preventiva:** La solución deberá incluir capacidades de detección y prevención de amenazas, control de dispositivos, análisis de comportamiento, protección de endpoints y gestión centralizada de la seguridad. Deberá contar con motores de análisis de alto rendimiento y tecnologías avanzadas de protección, incluyendo capacidades basadas en la nube para la identificación de amenazas emergentes y de día cero. Asimismo, deberá incorporar funcionalidades de control de acceso a la red que garanticen que todos los dispositivos conectados cumplan con las políticas de seguridad definidas, así como mecanismos de supervisión y control para la protección de la información, asegurando la prevención de fugas de datos y el cumplimiento de las políticas institucionales.
- **Protección completa de datos:** Garantiza la protección de datos contra las pérdidas accidentales. El escaneado de contenido integrado en el agente único garantiza que todos los datos confidenciales que transfieren los usuarios a dispositivos de almacenamiento extraíbles y a aplicaciones de Internet, como clientes de correo electrónico y mensajería instantánea, se detectan y se pueden auditar. El control granular de los dispositivos de almacenamiento extraíbles posibilita permitir el uso de dispositivos específicos, aplicar el uso de dispositivos cifrados o simplemente permitir un acceso de sólo lectura.

Como parte del fortalecimiento de la seguridad del ICANH, se requiere la adquisición de un software de gestión de vulnerabilidades basado en riesgos, dicho software ayuda a identificar cuales riesgos ponen en peligro real los procesos de negocio e identifica los activos que están fuera del monitoreo real. Actualmente, la identificación de superficie de ataque de los servicios crece debido al avance tecnológico y desde la oficina de tecnologías de la entidad, se realizan procesos manuales los cuales conllevan muchas veces a dejar brechas abiertas. La adquisición del software nos permitirá automatizar la detección de fallos de seguridad en tiempo real, priorizando aquellos que realmente detendrían la operación de los servicios. No solo se reduciría el riesgo de un ciberataque costoso, sino que la entidad se alinearía y daría cumplimiento a los estándares y controles de la ISO 27001:2022 de acuerdo a los lineamientos de MINTIC.

Descrito lo anterior, implementar una herramienta especializada en análisis de vulnerabilidades es fundamental para optimizar la eficiencia operativa del equipo de TI, eliminando la carga de búsqueda manual y proporcionando una hoja de ruta clara para la remediación basada en riesgos reales. Esta automatización no solo garantiza un inventario de activos siempre actualizado y preciso, sino que permite al personal técnico de seguridad centrarse en la resolución estratégica de fallos críticos, mejorando el tiempo de respuesta y asegurando que los recursos de seguridad se apliquen donde el impacto es mayor. Este software deberá permitir la identificación, evaluación y remediación de brechas de seguridad en la infraestructura tecnológica de la entidad, abarcando componentes como la seguridad perimetral, servidores, aplicaciones, sistemas de información, activos digitales, entre otros.

	PROCEDIMIENTO GESTIÓN PRECONTRACTUAL	CÓDIGO:	GC-PR-08-FO-10
		VERSIÓN:	01
	FORMATO FICHA TÉCNICA DE CONDICIONES ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN	FECHA:	10-01-2024

Así mismo, la solución deberá facilitar la generación, lectura y descarga de reportes de seguridad, con el fin de brindar una visión integral del estado de los distintos activos tecnológicos.

2) Solución Red Inalámbrica

De manera paralela, la Oficina de Tecnologías, debe garantizar el acceso a Internet inalámbrico, dado que este servicio es fundamental para asegurar una gestión institucional eficiente y de calidad, facilitando el trabajo colaborativo entre funcionarios y demás colaboradores de la entidad.

Desde el punto de vista de las comunicaciones, las redes inalámbricas se han consolidado como un componente esencial, ya que las organizaciones requieren, cada vez más, incrementar la productividad, mejorar la experiencia de los usuarios, y brindar canales de comunicación inmediata, además del intercambio de información en tiempo real.

El uso de la tecnología inalámbrica como medio de transmisión ha transformado significativamente las redes, especialmente en entornos donde no es posible implementar conexiones físicas. Por estas razones, la implementación y mantenimiento de una red inalámbrica robusta resulta indispensable para garantizar una adecuada interconexión tanto interna como externa.

La necesidad no corresponde a la adquisición de una nueva red inalámbrica, sino a la continuidad operativa de la infraestructura existe. El ICANH cuenta con una arquitectura de red inalámbrica compuesta por veinte (20) dispositivos de acceso (Access Points) distribuidos en la sede misional, sede administrativa y la sede Gregorio Hernández de Alba. Estos dispositivos operan bajo un modelo de gestión centralizada en la nube, lo que permite el monitoreo, soporte, actualizaciones de firmware y control de acceso de manera unificada.

La renovación del licenciamiento es necesaria debido a que la infraestructura de hardware instalada requiere de una suscripción activa para habilitar su plataforma de orquestación y mando original. Técnicamente, la compatibilidad se justifica bajo los siguientes criterios:

- Los puntos de acceso actualmente en operación utilizan protocolos de comunicación y aprovisionamiento específicos que solo son reconocidos por su consola de administración nativa en la nube. La falta de renovación de estas licencias inhabilitaría la capacidad de gestionar configuraciones y realizar el monitoreo de la red.
- Para garantizar la interoperabilidad, el licenciamiento debe ser totalmente compatible con el firmware y la arquitectura lógica de los equipos instalados. El uso de una solución de gestión distinta implicaría la incompatibilidad técnica del hardware actual, conllevando a la pérdida de la inversión realizada y la necesidad de sustituir la totalidad de los equipos físicos.
- El licenciamiento garantiza el acceso a parches de seguridad y actualizaciones críticas. Dado que los dispositivos actuales están vigentes, la renovación permite extender su vida útil bajo los estándares de protección institucional, evitando riesgos de vulnerabilidades por obsolescencia lógica.

Por lo expuesto, se requiere la renovación de la licencia de administración para los veinte (20) activos de red inalámbrica, asegurando así la continuidad del servicio, la administración centralizada y la protección de la inversión tecnológica de la entidad.

 ICANH	PROCEDIMIENTO GESTIÓN PRECONTRACTUAL		CÓDIGO:	GC-PR-08-FO-10
			VERSIÓN:	01
	FORMATO FICHA TÉCNICA DE CONDICIONES ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN		FECHA:	10-01-2024

3) Certificado de seguridad SSL

Adicionalmente la entidad requiere adquirir un certificado digital SSL/TLS de tipo OV Wildcard para el dominio *.icanh.gov.co, con el fin de garantizar la seguridad, confidencialidad e integridad de las comunicaciones digitales de la entidad y dar cumplimiento a los hallazgos identificados en el análisis de vulnerabilidades realizado durante el primer trimestre del año 2026 sobre la infraestructura tecnológica.

La ausencia de un certificado digital válido y reconocido genera, entre otros, los siguientes problemas operativos y de seguridad:

- Alertas de seguridad en los navegadores de los usuarios internos que acceden a los servicios web de la entidad, afectando la credibilidad institucional y la experiencia de usuario en los ambientes preproductivos.
- Imposibilidad de garantizar la autenticidad del servidor ante los clientes, lo que abre la posibilidad de ataques de tipo Man-in-the-Middle (MitM) que comprometan la confidencialidad de las credenciales y la información transmitida.
- La falta de certificado de seguridad afectaría los estándares y buenas prácticas de seguridad, como NIST SP y OWASP, que exigen el uso de certificados emitidos por autoridades certificadoras reconocidas. Su implementación daría cumplimiento al marco normativo colombiano en la Ley 527 de 1999, la Política de Gobierno Digital, el CONPES 3995 de 2020 - Política Nacional de Confianza y Seguridad Digital, y los controles del Modelo de Seguridad y Privacidad de la Información - MSPI del MinTIC
- Imposibilidad de acceder al firewall perimetral a través de su nombre DNS sin error de certificado, lo que obliga a los administradores a acceder por IP directa, reduciendo la trazabilidad y el control de acceso.
- Incapacidad de implementar políticas de HSTS (HTTP Strict Transport Security) sin un certificado válido, dejando expuestos los servicios web a ataques de degradación de protocolo.

La implementación del certificado digital se enmarca en el cumplimiento de los lineamientos de Gobierno Digital y de confianza digital del Estado colombiano, orientados a garantizar la seguridad de los servicios digitales y la protección de la información. En este contexto, la adquisición de un certificado SSL/TLS tipo OV Wildcard para el dominio *.icanh.gov.co se constituye como la solución técnicamente idónea, al permitir asegurar de manera centralizada todos los subdominios, fortalecer los mecanismos de autenticación y cifrado, y optimizar la gestión operativa de los certificados, por las siguientes razones:

a) Cobertura unificada de múltiples activos: Un único certificado Wildcard cubre todos los subdominios de primer nivel bajo icanh.gov.co, incluyendo el portal web institucional, el firewall perimetral administrado por nombre DNS, los portales de preproducción y otros, y cualquier nuevo servicio que se implemente durante la vigencia del contrato, sin incurrir en costos adicionales.

b) Validación de organización (OV) requisito de identidad institucional: La validación OV garantiza que el nombre "Instituto Colombiano de Antropología e Historia" quede inscrito en el certificado, permitiendo a los ciudadanos y usuarios verificar la autenticidad de los servicios digitales de la entidad. Esto supera las garantías de un certificado para el dominio y subdominios de la entidad, alineándose con los principios de transparencia y confianza digital exigidos a las entidades del Estado colombiano.

 ICANH	PROCEDIMIENTO GESTIÓN PRECONTRACTUAL	CÓDIGO:	GC-PR-08-FO-10
		VERSIÓN:	01
	FORMATO FICHA TÉCNICA DE CONDICIONES ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN	FECHA:	10-01-2024

c) Resolución del hallazgo del firewall perimetral: El firewall institucional actualmente genera errores de certificado al ser accedido mediante su nombre DNS, lo que obliga a los administradores a usar la dirección IP directa. La instalación del certificado Wildcard en el firewall resuelve este hallazgo operativo y mejora la postura de seguridad del acceso administrativo remoto.

En consecuencia, y conforme a lo anteriormente expuesto, la Oficina de Tecnologías debe velar por el adecuado funcionamiento de la plataforma tecnológica del ICANH. En tal sentido, la renovación del licenciamiento requerido obedece a la necesidad de garantizar la continuidad operativa de la infraestructura tecnológica, asegurando la compatibilidad, integración y correcto funcionamiento con las soluciones actualmente implementadas. La sustitución de estas herramientas implicaría riesgos asociados a la indisponibilidad de servicios, reprocesos técnicos, costos adicionales de migración y posibles afectaciones a la seguridad de la información institucional

Conforme a lo descrito, se hace necesario adelantar la renovación del licenciamiento correspondiente al equipo de seguridad perimetral (Firewall) y al sistema antivirus, la adquisición del software de análisis de vulnerabilidades, la adquisición de un certificado SSL OV Wildcard para *.icanh.gov.co y la renovación de la solución inalámbrica. La no ejecución del presente proceso de contratación podría generar riesgos asociados a la indisponibilidad de los servicios tecnológicos, exposición a vulnerabilidades de seguridad, pérdida o alteración de la información y afectación en la operación institucional.

La modalidad de Selección Abreviada mediante Subasta Inversa Electrónica es la que resulta procedente para el presente proceso contractual, teniendo en cuenta que la necesidad corresponde principalmente a la renovación y adquisición de licenciamientos tecnológicos, certificados digitales y servicios asociados que pueden ser definidos mediante especificaciones técnicas mínimas, objetivas, verificables y comparables en el mercado. En ese sentido, una vez acreditado el cumplimiento de los requisitos técnicos, de compatibilidad, vigencia, soporte y entrega exigidos por la entidad, el factor económico puede constituirse en el criterio determinante para la selección, garantizando pluralidad, transparencia y eficiencia en el gasto público, cuyas especificaciones técnicas, condiciones de desempeño y estándares de calidad pueden ser objetivamente definidos y comparables entre los diferentes oferentes del mercado. En consecuencia, la escogencia del contratista puede adelantarse mediante un procedimiento simplificado que garantice eficiencia, economía y selección objetiva, conforme a lo previsto en la Ley 1150 de 2007 y el Decreto 1082 de 2015.

Así mismo, la Entidad efectuó el análisis correspondiente frente a los mecanismos de adquisición disponibles, verificando que actualmente no existen Acuerdos Marco de Precios vigentes administrados por Colombia Compra Eficiente que satisfagan las necesidades técnicas relacionadas con licencias de firewall, antivirus, IPV6 y Access Point requeridas para el fortalecimiento de la seguridad tecnológica institucional. En este sentido, y en cumplimiento de lo establecido en el artículo 2.2.1.2.1.2.12 del Decreto 1082 de 2015, modificado por el Decreto 310 de 2021, se concluye que la Subasta Inversa Electrónica constituye el mecanismo más adecuado para garantizar condiciones de competencia y optimización de recursos públicos.

La utilización de esta modalidad de selección asegura además la observancia de los principios que rigen la contratación estatal, especialmente los de transparencia, igualdad, selección objetiva y libre concurrencia, permitiendo la participación de todos los interesados que acrediten las condiciones habilitantes exigidas. De igual forma, el procedimiento promueve la obtención de mejores condiciones económicas para la Entidad, mediante la puja dinámica de precios entre oferentes, garantizando una contratación eficiente y ajustada a las necesidades institucionales.

	PROCEDIMIENTO GESTIÓN PRECONTRACTUAL	CÓDIGO:	GC-PR-08-FO-10
		VERSIÓN:	01
	FORMATO FICHA TÉCNICA DE CONDICIONES ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN	FECHA:	10-01-2024

En atención a los lineamientos de optimización de recursos en la contratación pública, la presente contratación busca garantizar la continuidad de soluciones tecnológicas ya implementadas, evitando reprocesos, costos de migración, indisponibilidad de servicios y adquisición de herramientas redundantes.

3. OBJETO CONTRACTUAL

Adquirir la renovación de las licencias del equipo de seguridad perimetral y antivirus y renovación de las licencias de los dispositivos Access Point, y certificado SSL para el Instituto Colombiano de Antropología e Historia.

4. GENERALIDADES DEL PROCESO

Dada la naturaleza de la infraestructura existente (referencias XGS4300 para seguridad perimetral y dispositivos de acceso inalámbrico administrados en nube), la contratación tiene por objeto garantizar la continuidad operativa y la protección de la inversión realizada por la Entidad

El contrato planteado obedece a la necesidad de la entidad en renovar el licenciamiento de los siguientes servicios tecnológicos:

LOTE 1: Seguridad perimetral, antivirus y gestión de vulnerabilidades.

Licenciamiento firewall y antivirus de la solución actual vence el 10 de septiembre del 2026, así las cosas, a continuación, se relacionan los requerimientos para la presente contratación:

ÍTEM	LICENCIA	Cantidad Mínima	Tiempo	Fecha de vencimiento
1	Central Intercept X Advanced with XDR - 12 MOS - RENEWAL - GOV	230	12 meses	10/09/2026
2	Central Intercept X Advanced for Server with XDR - SERVERS - 12 MOS - RENEWAL - GOV	5	12 meses	10/09/2026
3	XGS4300 Email Protection - 12 MOS - RENEWAL (SKU: XM4C1CTAA)	1	12 meses	03/02/2027
4	XGS4300 Webserver Protection - 12 MOS - RENEWAL (SKU: XS4C1CTAA)	1	12 meses	03/02/2027
5	Xstream Protection for XGS4300 - 12 MOS - RENEWAL (SKU: XF4C1CTES)	1	12 meses	30/01/2027

 ICANH	PROCEDIMIENTO GESTIÓN PRECONTRACTUAL		CÓDIGO:	GC-PR-08-FO-10
			VERSIÓN:	01
	FORMATO FICHA TÉCNICA DE CONDICIONES ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN		FECHA:	10-01-2024

Descripción	Características técnicas Mínimas
Central Intercept X Advanced with XDR - 230 USERS - 12 MOS - RENEWAL – GOV	✓ Detección de procesos de encriptación maliciosos. ✓ Bloqueo de ataques Ransomware ✓ Bloqueo de propagación en la red ✓ Prevención de Ransomware de registro de arranque maestro y basado en archivos. ✓ Información detallada posterior a la limpieza, para que pueda ver dónde entró la amenaza. ✓ Incluir actualizaciones automáticas de las listas de definiciones de virus a partir de una ubicación en nube. ✓ Tener un control de periféricos.
XGS4300 Email Protection	✓ Protección y control de correo electrónico. ✓ Gestión de cuarentena de correo electrónico. ✓ Cifrado de correo electrónico y DLP. ✓ Registro e informes.
XGS4300 Web Protection and Enhanced Support	✓ Control de aplicaciones sincronizado. ✓ Protección y Control Web. ✓ Protección y control de aplicaciones. ✓ Visibilidad de aplicaciones en la nube. ✓ Conformación de tráfico web y de aplicaciones.
XGS4300 Webserver Protection	✓ Protección de firewall de aplicaciones web. ✓ Registro e informes
Xstream Protection for XGS4300	✓ Licencia base, protección de red. ✓ Protección de día cero. ✓ Orquestación central y soporte mejorado.

Nota: La renovación deberá activarse a partir del vencimiento de cada licencia actualmente vigente, garantizando que no exista interrupción del servicio ni pérdida de cobertura.

Licencia **Tenable Vulnerability Management (Nessus)** para gestión de vulnerabilidades, así como, la transferencia de conocimiento del uso de esta herramienta, así las cosas, a continuación, se relacionan los requerimientos:

ÍTEM	REQUERIMIENTO	Cantidad Mínima	Tiempo	Fecha de vencimiento
1	Nessus Professional includes vulnerability assessment, configuration assessment and malware detection. Nessus Professional - On Premise - Annual Subscription	1	12 meses	10/10/2026
2	Advanced Support for a Nessus Professional License.	12 horas	NA	

	PROCEDIMIENTO GESTIÓN PRECONTRACTUAL	CÓDIGO:	GC-PR-08-FO-10
		VERSIÓN:	01
	FORMATO FICHA TÉCNICA DE CONDICIONES ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN	FECHA:	10-01-2024

Se requiere la suscripción para la gestión de vulnerabilidades sobre la plataforma tecnológica actualmente en operación en la Entidad (basada en tecnología Nessus/Tenable), así como la transferencia de conocimiento en su uso avanzado. Esta elección se fundamenta en la necesidad de garantizar la trazabilidad histórica de las vulnerabilidades detectadas en vigencias anteriores, permitiendo el análisis de tendencias de riesgo sin pérdida de datos. Asimismo, la continuidad técnica evita procesos críticos de redimensionamiento, la reinstalación de agentes de escaneo en los servidores institucionales y el desgaste administrativo de una nueva curva de aprendizaje, asegurando así el máximo aprovechamiento de la infraestructura lógica ya desplegada

LOTE 2: Solución Red Inalámbrica

Renovar el licenciamiento de la plataforma de administración en la nube y de los equipos Access Point, que soportan la conectividad de las sedes Misional, Administrativa y Gregorio Hernández de Alba, cuya fecha de vencimiento se encuentra establecida para el 25 de diciembre de 2026, con el fin de garantizar la continuidad, disponibilidad y correcta operación del servicio de red inalámbrica

Renovar la licencia de la administración WiFi en nube y veinte (20) Access Point instalados en las sedes Misional, Administrativa y Gregorio Hernández de Alba del Instituto Colombiano de Antropología e Historia, el proponente, debe presentar la propuesta técnica que incluya:

Renovar el licenciamiento de la solución inalámbrica de la entidad Cloud Management (iMaster NCE-Campus) para Administración en la nube - Subscription License, AirEngine-Indoor, Per Device, 1 Year - Para las 20 licencias de los dispositivos Access Point:

2102353VUR10PB100533
2102353VUR10PB106319
2102353VUR10PB106321
2102353VUR10PB106312
2102353VUR6RMB014643
2102353VURW0MB013823
2102353VURW0MB013489
2102353VURW0MB013492
2102353VUR10PB106320
2102353VUR10PB106318
2102353VUR10PB106317
2102353VUR10PB100615
2102353VUR10PB100630
2102353VUR10PB100646
2102353VUR10PB100532
2102353VUR10PB100624
2102353VUR10PB100622
2102353VUR10PB100620
2102353VUR10PB100522
2102353VUR10PB100631

Renovar 20 licencias para equipos Access Point AirEngine5761-11 (11ax indoor, 2+2 dual bands, smart antenna, USB, BLE)_Hi-Care Basic AirEngine5761-11 Serial:

	PROCEDIMIENTO GESTIÓN PRECONTRACTUAL	CÓDIGO:	GC-PR-08-FO-10
		VERSIÓN:	01
	FORMATO FICHA TÉCNICA DE CONDICIONES ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN	FECHA:	10-01-2024

Renovar la licencia de la administración WiFi en nube y veinte (20) Access Point instalados en las sedes Misional, Administrativa y Gregorio Hernández de Alba del Instituto Colombiano de Antropología e Historia, el proponente, debe presentar la propuesta técnica que incluya:

2102353VUR10PB100533
 2102353VUR10PB106319
 2102353VUR10PB106321
 2102353VUR10PB106312
 2102353VUR6RMB014643
 2102353VURW0MB013823
 2102353VURW0MB013489
 2102353VURW0MB013492
 2102353VUR10PB106320
 2102353VUR10PB106318
 2102353VUR10PB106317
 2102353VUR10PB100615
 2102353VUR10PB100630
 2102353VUR10PB100646
 2102353VUR10PB100532
 2102353VUR10PB100624
 2102353VUR10PB100622
 2102353VUR10PB100620
 2102353VUR10PB100522
 2102353VUR10PB100631

LOTE 3: Certificado de seguridad SSL

Adquirir el certificado digital SSL/TLS para el dominio y subdominios de *.icanh.gov.co, cuya vigencia actual finaliza el 30 de octubre de 2026, de conformidad con los requerimientos técnicos y de seguridad definidos por la entidad, con el fin de garantizar la continuidad en la protección de las comunicaciones y servicios asociados.

ÍTEM	REQUERIMIENTO	Cantidad Mínima	Tiempo
1	Certificado SSL Wildcard OV	1	2 años

4.1. TIEMPOS ESTIMADOS

El proceso de renovación de licencias y la adquisición del certificado digital deberá completarse de manera previa a su fecha de vencimiento, incluyendo, cuando aplique, la gestión de cambio de proveedor desde la plataforma de administración. En este sentido, el proveedor deberá garantizar la continuidad del servicio, asegurando la disponibilidad, correcta activación y plena operatividad de las licencias renovadas, así como la emisión oportuna del certificado digital. De igual forma, deberá asegurar la prestación del soporte técnico asociado a dichos servicios durante el período contratado, evitando cualquier afectación en la operación.

 ICANH	PROCEDIMIENTO GESTIÓN PRECONTRACTUAL	CÓDIGO:	GC-PR-08-FO-10
		VERSIÓN:	01
	FORMATO FICHA TÉCNICA DE CONDICIONES ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN	FECHA:	10-01-2024

5. ESPECIFICACIONES TÉCNICAS REQUERIDAS

LOTE No. 1: Seguridad Perimetral, Antivirus y Gestión de Vulnerabilidades.

ESPECIFICACIONES TÉCNICAS MINIMAS REQUERIDAS:

1.1 Licenciamiento de seguridad Endpoint

- Renovación para el ICANH de doscientas treinta (230) licencias del antivirus Central Intercept X Advanced with XDR Includes Choice por el término de un (1) año.
- Renovación del licenciamiento de cinco (5) servidores mediante Central Managed Detection and Response Server por el término de un (1) año.
- Renovación de una (1) licencia Central Intercept X Advanced with XDR por el término de un (1) año.

1.2 Seguridad perimetral

- Renovación de la suscripción XSTREAM PROTECTION para el equipo XGS4300 instalado en la red del ICANH, incluyendo Web Protection y Enhanced Support, por el término de un (1) año.
- Renovación de la suscripción XGS4300 Email Protection por el término de un (1) año.
- Renovación de la suscripción XGS4300 Webserver Protection por el término de un (1) año.

1.3 Gestión de vulnerabilidades

- Suministro, instalación y configuración de la solución Tenable Vulnerability Management (Nessus), incluyendo licencia y soporte por un (1) año.

OBLIGACIONES DEL CONTRATISTA:

- Garantizar soporte técnico en sitio cuando sea requerido por el ICANH.
- Prestar soporte remoto mediante canales telefónico, correo electrónico y sistema de tickets vía web.
- Garantizar el escalamiento de casos no resueltos directamente al fabricante.
- Proporcionar el recurso humano y tecnológico necesario para la atención y recuperación de incidentes de seguridad que afecten la operación de la entidad.
- Revisar y afinar las reglas de seguridad actualmente implementadas en la red del ICANH.
- Designar un representante para coordinar las acciones entre el ICANH y el contratista dentro de los tres (3) días siguientes a la suscripción del contrato.
- Suscribir y cumplir el acuerdo de confidencialidad definido por el ICANH.
- Prestar soporte y asistencia técnica virtual para la herramienta Nessus durante la vigencia contractual.
- Presentar informe detallado del estado actual de configuración de reglas y políticas de seguridad web, incluyendo hallazgos, recomendaciones y plan de remediación.
- Realizar doce (12) horas de transferencia de conocimiento en modalidad virtual para máximo tres (3) funcionarios del ICANH sobre administración y uso de Nessus.

ENTREGABLES:

- Documento expedido por el fabricante que acredite la propiedad del licenciamiento antivirus a nombre del ICANH por un (1) año.

	PROCEDIMIENTO GESTIÓN PRECONTRACTUAL	CÓDIGO:	GC-PR-08-FO-10
		VERSIÓN:	01
	FORMATO FICHA TÉCNICA DE CONDICIONES ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN	FECHA:	10-01-2024

- Documento expedido por el fabricante que acredite la propiedad del licenciamiento Nessus a nombre del ICANH por un (1) año.
- Informe de configuración y parametrización de la herramienta Nessus.
- Documento con:
 - canales de soporte,
 - horarios de atención,
 - procedimiento de escalamiento,
 - niveles de soporte.

LOTE No. 2 - Solución Red Inalámbrica.

ESPECIFICACIONES TÉCNICAS MINIMAS REQUERIDAS:

- Renovación por un (1) año del licenciamiento de la solución de red inalámbrica AirEngine-Indoor en nube.
- Renovación por un (1) año del licenciamiento de veinte (20) Access Point AirEngine5761-11.

OBLIGACIONES DEL CONTRATISTA:

- Garantizar soporte técnico remoto mediante teléfono, correo electrónico y sistema de tickets vía web.
- Garantizar escalamiento de incidentes al fabricante.
- Designar un representante de coordinación entre el ICANH y el contratista.

ACUERDOS DE NIVELES DE SERVICIO:

Nivel de Impacto	Descripción	Tiempo de solución (horas/días calendario)
Crítico	Afectación total del servicio de red inalámbrica en todas las sedes o en la mayoría de ellas.	4 horas calendario
Alto	Interrupción del servicio en una sede completa o en una zona crítica.	8 horas calendario
Medio	Falla en uno o varios AP (Access Point) que afecte parcialmente a un grupo de usuarios.	1 a 2 días
Bajo	Problemas intermitentes, baja señal o solicitudes menores que no interrumpen el servicio pero afectan la experiencia de usuario.	3 días

ENTREGABLES:

- Certificado del fabricante que acredite al proponente como distribuidor autorizado.

 ICANH	PROCEDIMIENTO GESTIÓN PRECONTRACTUAL	CÓDIGO:	GC-PR-08-FO-10
		VERSIÓN:	01
	FORMATO FICHA TÉCNICA DE CONDICIONES ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN	FECHA:	10-01-2024

- Documento expedido por el fabricante que certifique la propiedad del licenciamiento de la controladora y Access Point a nombre del ICANH.

LOTE No. 3 – Certificado Digital SSL

ESPECIFICACIONES TÉCNICAS MINIMAS REQUERIDAS:

- Emisión de certificado digital SSL OV Wildcard para *.icanh.gov.co con vigencia de dos (2) años.
- Compatibilidad con TLS 1.2 y TLS 1.3.
- Algoritmo RSA mínimo de 2048 bits (preferible 4096) o ECDSA P-256.
- Hash SHA-256 mínimo.
- Inclusión de la CA en almacenes raíz Mozilla, Microsoft y Apple.
- Entrega en formatos:
- PEM (.crt/.pem),
- PKCS#12 (.pfx),
- DER,
- CA-bundle.
- Reemisiones ilimitadas durante la vigencia del certificado.

OBLIGACIONES DEL CONTRATISTA:

- Brindar acompañamiento técnico para la instalación del certificado en el firewall XGS4300 cuando sea requerido.
- Garantizar reemisiones ilimitadas sin costo adicional.
- Prestar soporte técnico durante toda la vigencia del certificado.
- Notificar al supervisor del contrato con mínimo sesenta (60) días de anticipación al vencimiento.

ENTREGABLES:

- Certificado digital en todos los formatos requeridos por la entidad.
- Documento oficial de expedición del certificado indicando:

Fecha de emisión,
fecha de vencimiento,
vigencia,
tipo de certificado,
garantía de renovación.

6. LUGAR DE EJECUCIÓN

La prestación del servicio objeto de la presente contratación se realizará de acuerdo con las especificaciones que determine el Supervisor del contrato, las cuales se desarrollarán en el domicilio contractual de las sedes Principal, Administrativa y el Edificio Nuevo del Instituto Colombiano de Antropología e Historia, en la ciudad de Bogotá D.C.

 ICANH	PROCEDIMIENTO GESTIÓN PRECONTRACTUAL	CÓDIGO:	GC-PR-08-FO-10
		VERSIÓN:	01
	FORMATO FICHA TÉCNICA DE CONDICIONES ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN	FECHA:	10-01-2024

7. FASES DE LA EJECUCIÓN CONTRACTUAL

A continuación, se presenta las actividades principales que se contemplan para la ejecución contractual:

7.1. FASE INICIAL

- **LOTE 1: Seguridad Perimetral, Antivirus y Gestión de Vulnerabilidades.**
 - Realizar la renovación de licencias ya existentes del equipo Firewall y antivirus de acuerdo a las especificaciones técnicas solicitadas en la presente ficha técnica.
 - Entregar, instalar, configurar y colocar en funcionamiento un software Nessus para la gestión de vulnerabilidades, incluyendo la licencia de soporte por un (1) año.
- **LOTE 2: Solución Red Inalámbrica**
 - Realizar la renovación de las licencias de la solución WIFI renovada de acuerdo a las especificaciones técnicas solicitadas en la presente ficha técnica.
- **LOTE 3: Certificado de seguridad SSL**
 - La entidad deberá coordinar con el proveedor el inicio del proceso de validación OV (Organization Validation), proporcionando la documentación legal de la entidad requerida por la Autoridad Certificadora para la verificación de la organización. El proveedor deberá iniciar el trámite 15 días antes del vencimiento del certificado actual.

7.2. FASE DE DESARROLLO

- **LOTE 1: Seguridad Perimetral, Antivirus y Gestión de Vulnerabilidades.**
 - Entregar la documentación correspondiente a los soportes de renovación del licenciamiento contratado por la entidad.
- **LOTE 2: Solución Red Inalámbrica**
 - Realizar la entrega de la documentación que derive de las licencias a nombre del ICANH de la solución WIFI.
- **LOTE 3: Certificado de seguridad SSL**
 - Realizar la entrega de un documento que certifique la expedición del certificado digital a nombre de la entidad.
 - Garantizar la renovación del certificado para el segundo año asegurando que este se realice antes de su expiración.

7.3. FASE DE FINALIZACIÓN

La Entidad hará uso de las licencias, certificados y demás componentes adquiridos mediante la presente ficha técnica durante el período solicitado en la misma. Asimismo, se garantiza la disponibilidad del

 ICANH	PROCEDIMIENTO GESTIÓN PRECONTRACTUAL		CÓDIGO:	GC-PR-08-FO-10
			VERSIÓN:	01
	FORMATO FICHA TÉCNICA DE CONDICIONES ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN		FECHA:	10-01-2024

soporte técnico asociado durante todo el tiempo requerido, en concordancia con la vigencia de las licencias y certificados, conforme a las condiciones establecidas por el proveedor.

8. INFORMES Y/O REPORTES

- **LOTE 1: Seguridad Perimetral, Antivirus y Gestión de Vulnerabilidades.**
 - Entregar documentos que certifique por el fabricante el licenciamiento renovado a nombre del ICANH.
 - Presentar un informe detallado del estado actual de configuración de las reglas y políticas de seguridad web en la infraestructura de seguridad perimetral, incluyendo el análisis de hallazgos, recomendaciones técnicas para su fortalecimiento y un plan de trabajo estructurado para la remediación de las brechas identificadas en el análisis.
 - Entregar el informe de instalación, configuración y parametrización del software Nessus.
- **LOTE 2: Solución Red Inalámbrica**
 - Entregar documentos que certifique por el fabricante el licenciamiento renovado a nombre del ICANH.
- **LOTE 3: Certificado de seguridad SSL**
 - Entregar todos los documentos y soportes que derive de la adquisición del certificado digital a nombre de la entidad y la garantía de renovación del certificado de su segundo año antes de su vencimiento.

9. PERSONAL MÍNIMO DE TRABAJO

LOTE 1: Seguridad Perimetral, Antivirus y Gestión de Vulnerabilidades.

El proponente debe presentar como mínimo dos (2) Ingenieros certificados en o “Sophos Certified Architect – XG Firewall”, para brindar soporte técnico y capacitación de acuerdo a las necesidades de la entidad. Los requerimientos para estos dos ingenieros son los siguientes:

1) Formación académica:

- Profesional en ingeniería de sistemas, software, telecomunicaciones o afines.

2) Experiencia:

- Ingeniero No. 1: debe presentar certificaciones de experiencia emitidas por usuario final cuya sumatoria sea igual o superior a tres (3) años de experiencia en Colombia en soporte técnico de soluciones.
- Ingeniero No. 2: debe presentar certificaciones emitidas por usuario final cuya sumatoria sea igual o superior a tres (3) años de experiencia en Colombia en Seguridad Informática.

 ICANH	PROCEDIMIENTO GESTIÓN PRECONTRACTUAL		CÓDIGO:	GC-PR-08-FO-10
			VERSIÓN:	01
	FORMATO FICHA TÉCNICA DE CONDICIONES ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN		FECHA:	10-01-2024

Se deberá anexar copia del diploma, hoja de vida, tarjeta profesional y certificado de vigencia de la tarjeta profesional y demás documentos requeridos de los ingenieros, con sus respectivos soportes, dentro del proceso de evaluación técnica y selección.

Los profesionales que conformen el equipo de trabajo deberán contar con una experiencia mínima de tres (3) años, la cual deberá estar debidamente certificada y reflejada en la hoja de vida, especialmente en actividades relacionadas con el manejo de equipos de seguridad y soluciones antivirus de acuerdo a la solución implementada en la entidad.

Asimismo, el personal deberá estar certificado en la marca de la solución de seguridad. Las certificaciones deben ser expedidas directamente por el fabricante o por un distribuidor mayorista autorizado.

Estos requisitos son indispensables para garantizar el nivel de especialización y la idoneidad técnica en la administración y soporte de dichas herramientas.

La Entidad se reserva el derecho de solicitar cualquier aclaración que considere necesaria con el fin de verificar el cumplimiento de los requerimientos de formación o experiencia solicitada.

Si por causas excepcionales no atribuibles al contratista, caso fortuito o fuerza mayor se hace necesario realizar una modificación o cambio de algún integrante del equipo de trabajo durante la ejecución del contrato, deberá ser aprobado por la entidad contratante, a través del supervisor del contrato, previa verificación del cumplimiento de los requisitos de cada perfil definido en la Ficha Técnica.

El adjudicatario debe garantizar que durante la ejecución del contrato cuente con todo el Equipo de Trabajo, por esta razón, al solicitar un cambio de profesional para determinado cargo, el contratista deberá entregar con la solicitud de cambio, la hoja de vida del candidato que cumpla el perfil requerido debidamente soportada, dando cumplimiento a las mismas o mejores calidades del profesional.

10. FORMA DE PAGO

El valor del contrato que resulte del presente proceso de selección se cancelará así:

LOTE 1: Seguridad Perimetral, Antivirus y Gestión de Vulnerabilidades.

1. Un (1) primer pago correspondiente al ochenta por ciento (80%) del valor total ofertado del LOTE 1 previo a las licencias renovadas del firewall y antivirus junto con la documentación que acrediten la propiedad del ICANH sobre dicho licenciamiento y el informe detallado del estado actual de configuración de las reglas y políticas de seguridad web en la infraestructura de seguridad perimetral.
2. Un segundo (2) pago correspondiente al veinte por ciento (20%) restante del valor total ofertado del LOTE 1 previa entrega de la licencia Nessus y la documentación solicitada (informes, documentación completa de la solución instalada y la transferencia de conocimiento).

LOTE 2: Solución Red Inalámbrica

Un (1) único pago correspondiente al cien por ciento (100%) del valor total ofertado del LOTE 2 sobre la solución de WIFI, previa entrega de las licencias que acrediten la propiedad del ICANH

 ICANH	PROCEDIMIENTO GESTIÓN PRECONTRACTUAL	CÓDIGO:	GC-PR-08-FO-10
		VERSIÓN:	01
	FORMATO FICHA TÉCNICA DE CONDICIONES ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN	FECHA:	10-01-2024

LOTE 3: LOTE 3: Certificado de seguridad SSL

Un (1) único pago correspondiente al cien por ciento (100%) del valor total ofertado del LOTE 3 una vez efectuada la adquisición del certificado SSL para el dominio y subdominios de la entidad, así mismo la entrega de la documentación que derive del trámite.

Todos los pagos se efectuarán previa presentación de la factura, informe, certificación en la que conste cumplimiento de las obligaciones frente al Sistema de Seguridad Social Integral en salud, pensión y riesgos laborales (en caso de ser persona natural), o acreditación de estar al día en el pago de obligaciones frente al Sistema de Seguridad Social Integral y Parafiscales (SENA, ICBF y Cajas de Compensación Familiar) (en caso de ser persona jurídica) y del certificado de cumplimiento a sistema a satisfacción expedido por el supervisor del contrato.

NOTA 1: Se aclara que, el acceso al sistema Olimpia incluido en precedencia, será concedido por el Ministerio de Hacienda y Crédito Público al Comitente Vendedor dentro de los tres (03) días hábiles siguientes a la generación de la factura electrónica.

El ICANH efectuará las retenciones que en materia tributaria tenga establecida la Ley y respecto de las cuales sea su obligación efectuar la retención. En los demás casos, el contratista deberá cumplir con el pago de los impuestos, tasas o contribuciones que se deriven de la presente contratación.

Deberán ser tramitadas por el contratista, las devoluciones o exenciones a que crea tener derecho ante la respectiva Administración de Impuestos, sin responsabilidad alguna por parte del ICANH o costo para ella.

Todos los impuestos, retenciones y gastos que se causen por razón de la legalización y ejecución de la presente contratación, incluidas la constitución de la garantía única de cumplimiento en caso de que se le requiera, son de cargo exclusivo del contratista. Por lo tanto, los precios que se propongan deberán considerar tales conceptos.

NOTA 2: Las facturas de venta o su equivalente para el pago deben ser presentadas en números enteros, sin decimales.

PARÁGRAFO: Los pagos de cada uno de los ítems anteriores se efectuarán dentro del plazo establecido, efecto para el cual el comitente comprador adelantará los trámites pertinentes para realizar el pago dentro de dicho término.



JONATHAN ANDRÉS SÁNCHEZ CORREDOR
JEFE OFICINA DE TECNOLOGÍAS

Elaboró: Sandra Silva – Profesional Especializada, Oficina de Tecnologías *Sandra Silva*
Revisó: Paola Rodas – Abogada Contratista, Oficina de Tecnologías *Paola Rodas*