EL INSTITUTO NACIONAL DE CANCEROLOGIA – EMPRESA SOCIAL DEL ESTADO, INVITA A PRESENTAR PROPUESTAS PARA CONTRATAR LOS SERVICIOS DE OUTSOURCING EN TECNOLOGÍA INFORMÁTICA, QUE INCLUYE EL ARRENDAMIENTO DE EQUIPOS DE IMPRESIÓN Y ESCANEO, EQUIPOS DE CÓMPUTO, SERVICIOS DE INFRAESTRUCTURA Y SEGURIDAD, MESA DE AYUDA, LICENCIAMIENTO, SUMINISTROS E INSUMOS, ACORDE CON LOS PRESENTES TÉRMINOS DE CONDICIONES, SUS ANEXOS Y EL CONTRATO QUE SE CELEBRE PARA EL EFECTO, MEDIANTE SUBASTA INVERSA PRESENCIAL.

ANEXO 3. ANEXO TÉCNICO

A continuación, se detallan las especificaciones que el proponente debe tener en cuenta para presentar su oferta, la cual debe estar directamente relacionada con el objeto de esta invitación, la información que se detalla adelante y las consideraciones de todo orden que estime, para ofrecer mejores condiciones al INC.

1. DESCRIPCIÓN GENERAL DEL SERVICIO

Se requiere suscribir un contrato con un proveedor para que brinde el servicio de Outsourcing en Tecnología Informática, considerando equipos de cómputo, servidores, licenciamiento, equipos y servicios de impresión, administración física y lógica de redes de voz y datos, comunicaciones alámbricas e inalámbricas, administración de servidores y sistemas de almacenamiento, administración de los servicios de correo electrónico, dominio, administración de servicios Windows y Linux, servicios de red y monitoreo, seguridad informática incluyendo seguridad perimetral, Seguridad Endpoint, Seguridad de Redes, Seguridad Criptográfica, Seguridad Email, y autenticación, incluido hardware, software, gestión de operaciones TI, incluidos los servicios de implementación, configuración, migración de información, estabilización, administración de la infraestructura, soporte 7x24 con personal técnico calificado y gerencia de proyecto; mantenimiento preventivo y correctivo, gestión de garantías, gestión de inventarios, suministro de papel, repuestos e insumos, que se requieran en el Instituto Nacional de Cancerología (INC), de acuerdo con las condiciones establecidas en este Anexo Técnico, la normatividad vigente y el contrato que se derive.

El objeto a contratar es fundamental para garantizar la gestión de la información en toda la Institución. Bajo la modalidad de Outsourcing, se busca optimizar los procesos de comunicaciones, impresión y procesamiento, garantizando la incorporación de infraestructura de cómputo e impresión nueva, acorde con las necesidades, y apoyada por un óptimo y permanente servicio de soporte a usuarios finales, todo ello bajo los más altos estándares de calidad, oportunidad y seguridad.

Bajo esta modalidad, se busca incrementar la disponibilidad de los servicios involucrados, disminuir los tiempos de atención a requerimientos reportados, eliminar costos de ocio por inoperancia en los equipos de tecnología informática, gestionando la capacidad instalada y manteniendo la continuidad de los servicios, contando con un excelente servicio al cliente, ejerciendo un control real en la operación y disminuyendo los costos relacionados mediante procesos de optimización bajo protocolos de servicio y uso, alineados a las mejores prácticas

1.1. Objetivos de la invitación

1.1.1. Objetivo General

Contratar los servicios de Outsourcing en Tecnología Informática, que incluye el arrendamiento de equipos de impresión y escaneo, equipos de cómputo, servicios de infraestructura y seguridad, mesa de ayuda, licenciamiento, suministros e insumos; de acuerdo con las condiciones establecidas y descritas en el Anexo Técnico 3, la normatividad vigente y el contrato que se derive.

1.1.2. Objetivos Específicos

1.1.2.1 Contar en la modalidad de Outsourcing con el servicio de impresión, incluido el hardware, software, productos y servicios conexos, detallados en este Anexo Técnico, que permita la optimización del sistema de impresión de usuarios finales.

1.1.2.2 Contar con el servicio de Outsourcing en Equipos de Cómputo, incluido el hardware y el software, productos y servicios conexos, detallados en este Anexo Técnico.

1.1.2.3 Contar con el servicio de Outsourcing en Equipos de Comunicaciones inalámbricas, incluido el hardware, software, productos y servicios conexos, detallados en este Anexo Técnico.

1.1.2.4 Contar con el servicio de Outsourcing en la gestión, operación y administración de las redes de voz y datos, incluidas comunicaciones alámbricas e inalámbricas.

1.1.2.5 Contar con el servicio de Outsourcing para la administración, soporte de los servicios de Correo electrónico, Firewall, Dominio, servicios de red (DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), AD (Active Directory), entre otros).

1.1.2.6 Garantizar al usuario la oportuna prestación del servicio, brindando una solución efectiva y a tiempo, en la atención de los requerimientos que surjan alrededor de la infraestructura de cómputo, impresión, comunicaciones alámbricas e inalámbricas, y suministro de insumos, que se contrate en la modalidad de Outsourcing.

1.1.2.7 Contar con un centro de servicio en las instalaciones del INC, que opere 7x24, que permita a los usuarios del Instituto acceso a un punto único de contacto, que cuente con infraestructura adecuada, con las herramientas que garanticen el registro, seguimiento, control y trazabilidad de los servicios requeridos y atendidos.

1.1.2.8 Contar con las herramientas de apoyo suficientes que garanticen una gestión de los servicios informáticos con calidad, que facilite la operación del punto único de contacto (Mesa de Ayuda), apoyado en software legalmente licenciado del cual pueda hacer uso el INC sin vulnerar derechos de autor que permita el registro eficiente, seguimiento, trazabilidad de incidentes, bajo las mejores prácticas fundamentadas en ITIL® (Information Technology Infraestructure Library). Debe implementarse una mesa de ayuda integral que registre y solucione las solicitudes de sistemas, y que registre y trámite las de otras áreas o servicios diferentes. El trámite de las solicitudes que no son de sistemas, incluye: recibir llamada, clasificar el servicio, registrar los datos de la solicitud, enviar la solicitud al área correspondiente; luego recibe el reporte de resolución y envía reporte al solicitante del estado de trámite. Se emitirán reportes permanentes del estado de avance de las solicitudes realizadas.

1.1.2.9 Contar en las instalaciones del INC, con personal calificado, para brindar el apoyo técnico que requiere la implementación y administración de los servicios referidos.

1.1.2.10 Garantizar la protección y seguridad informática del INC (Incluye seguridad perimetral, Seguridad Endpoint, Seguridad de Redes, Seguridad Criptográfica, Seguridad Email y autenticación)

1.2. Vigencia De La Oferta

El plazo estimado para la ejecución del contrato será de 35 meses. Se estiman dos meses iniciales para el proceso de transición y 33 meses para la etapa de operación. Contados a partir de la legalización del contrato. Por lo tanto, los valores ofertados por cada ítem o servicio, deberán mantenerse en sus características técnicas ofertadas y en el precio. Los presupuestos de los años 2020, 2021 y 2022, se manejarán a través de vigencias futuras.

1.3. Localización del Servicio

El servicio se prestará en la sede del Instituto Nacional de Cancerología, ubicada en la Calle 1 No. 9-85, en la ciudad de Bogotá, D.C. Se debe prestar los servicios del objeto contractual en la sede principal, Sede CPRED, ubicado en la Carrera 10 No. 1-59 y debe prestar soporte remoto en cualquier ubicación donde se encuentren los usuarios del Instituto.

2. CARACTERISTICAS GENERALES DEL SERVICIO

Para cada ítem el oferente debe indicar si su oferta cumple o no con el requerimiento en el archivo Anexo No. 7 TecnicosInvitacionPublica_Outsourcing.xlsx, en su pestaña RTG – Requisitos Técnicos Generales y realizar las observaciones que considere pertinente, en la pestaña EMR, Especificaciones Mínimas Requeridas.
El objeto a contratar debe incluir los equipos que se describen en las Tabla 1 y Tabla 2, el licenciamiento incluido en la Tabla 3 y los servicios conexos referidos en la Tabla 4, y cumpliendo con las especificaciones mínimas requeridas con iguales o superiores características, todas ellas detalladas en el Anexo No. 7 TecnicosInvitacionPublica_Outsourcing.xlsx.

En el transcurso de duración del contrato, el INC, podrá adicionar unidades de cualquier tipo de equipo, licencias que cumplan con las especificaciones técnicas mínimas, equivalentes o superiores las cuales deberán ser solicitadas por parte de la supervisión del contrato, bajo los precios acordados, conforme a las necesidades adicionales que el INC requiera. El contratista estará en la obligación de suministrar y atender dichos requerimientos. Dichas solicitudes no implicaran un modificatorio al contrato, a no ser que no se cuente con el presupuesto disponible en el mismo.

La oferta deberá considerar un valor de opción de compra sobre los equipos, dispositivos o periféricos, con excepción de los equipos de impresión equivalente a dos cuotas adicionales de arrendamiento después de terminado el contrato inicial. Dichas cuotas no harán parte del valor total de la oferta. El Instituto podrá o no hacer uso de la opción de compra para los equipos que considere conveniente.

El contratista deberá instalar, migrar la información y administrar los ítems que se detallan en este Anexo Técnico, dentro de los más altos estándares de calidad y oportunidad.

2.1. Especificaciones

Tabla 1: Equipos Modalidad Outsourcing

Descripción
Equipos de cómputo
Equipos de impresión
Equipos de escaneo
Lectores de código de barras
Servidores
Equipos comunicaciones alámbricas e inalámbricas
Equipos de seguridad informática

Tabla 2: Equipos Modalidad Administrados

Descripción
Equipos de cómputo – Escritorio, Portátiles Mini PC
Equipos de impresión
Servidores
Equipos comunicaciones alámbricas e inalámbricas

Tabla 3: Licenciamiento

Descripción
Ofimática Office 365 Licencias E3 – E1 – ProPlus
Antivirus para Endpoints y Servidores con soporte Windows, Linux y MAC
Data Lost Prevention para Endpoint + Data Lost Prevention para Office 365
Sistemas operativos de equipos y servidores
Licenciamiento Firewall Nueva Generación
Licenciamiento sistema de Analítica de eventos y detección de amenazas
Licenciamiento solución Antispam
Herramientas de monitoreo de red y disponibilidad servidores
Compresores de archivos RAR
Herramienta de Help Desk basada en ITIL
Herramienta de gestión de inventarios
Licenciamiento de servicios de nombres de Dominio – DNS
Licenciamiento Directorio activo bajo Windows en HA
Licenciamiento de servicio DHCP
Licenciamiento de servicio WSUS
Herramientas de virtualización
Herramientas de Backup y recuperación
Licencias de programa de soporte remoto
Licenciamiento Programas de gestión y control de Impresión
Herramienta de borrado seguro de información

Tabla 4: Servicios Conexos

Descripción
Gestión de servidores

Gestión de servicios de directorio activo y Dominio
Gestión de servicios de Redes de voz, datos y conectividad
Gestión de Seguridad Informática
Gestión de Operaciones TI

2.2. Actividades Generales que debe desarrollar el contratista

El Instituto Nacional de Cancerología requiere renovar el servicio de Outsourcing en equipos de cómputo, impresión, comunicaciones alámbricas e inalámbricas y la administración de infraestructura propiedad del INC.

El servicio debe contar con un esquema de trabajo apoyado por una mesa de ayuda, soporte en sitio, mantenimientos preventivos, correctivos, manejo de inventarios, control de garantías, control de licencias de software en uso, administración de redes, administración impresión, administración servidores, servicios administrados de seguridad informática, personal técnico y especializado en sitio, suficiente para garantizar un servicio de alta calidad.

Las principales actividades a desarrollar son las siguientes:

DIAGNÓSTICO. Establecer y mantener documentada la situación actual de los servicios de Outsourcing existentes y propuestos, e identificar la tecnología y los procedimientos que permitan garantizar disponibilidad, mejora del servicio y reducción de costos.

- HARDWARE. Instalar equipos, que cuenten con las especificaciones mínimas requeridas (EMR) y adecuadas a las necesidades de las diferentes áreas del INC, que cuenten con la contingencia que garantice la disponibilidad permanente del servicio, con los controles de inventarios requeridos.

- SOFTWARE: El Outsourcing, debe contar con el software adecuado que permita: (a) garantizar la operación de los servicios del INC, que corran sobre las plataformas ofertadas. (b) realizar la gestión de recursos físicos, operativos y de personal, (c) asegurar y custodiar la información que se genere a partir de los dispositivos, y herramientas a cargo, (d) generar estadísticas de la gestión de hardware y software, servicios conexos y personal, (e) administrar y gestionar la seguridad informática, (f) administrar software de mesa de ayuda, (g) gestionar y controlar inventarios en tiempo real, (h) gestionar y controlar impresiones, y apoyar políticas de cero papel, (i) administrar y monitorear de forma eficiente plataformas a cargo.

- LICENCIAS DE USO: El software debe estar licenciado y autorizado su uso para el Instituto Nacional de Cancerología. Este ítem incluye sistemas operativos, herramientas de administración, herramientas de ofimática, herramientas de seguridad informática, herramientas para compresión/descompresión de archivos, herramientas de gestión de mesa de ayuda, herramientas de control de inventarios, control de impresión entre otros, para los equipos, servidores y plataformas en las modalidades de Outsourcing y administrados.

- ALTA DISPONIBILIDAD: Implementar un servicio de Outsourcing que garantice servicios de alta disponibilidad para: (a) Servicios de dominio y directorio activo (b) servicio de impresión, (c) administración de la gestión de la red (d) monitoreo de todos los servicios (e) servicios de seguridad informática (f) servidores físicos de Outsourcing.

- SERVICIOS: El Outsourcing TI debe implantar, operar y mantener de manera continua los servicios de Gestión de servidores, Gestión de servicios de directorio activo y Dominio, Gestión de servicios de Redes de voz, datos y conectividad, Gestión de Seguridad Informática, Gestión de Operaciones TI.

- INSUMOS Y REPUESTOS: El Outsourcing debe garantizar la provisión de todos los insumos y repuestos requeridos sobre los equipos y dispositivos en Outsourcing o equipos administrados durante la vigencia del contrato.

- TALENTO HUMANO: El servicio debe ser prestado y ejecutado por personal profesional y técnico calificado y con experiencia previa en la labor a desempeñar en el INC. Las hojas de vida y los certificados del personal que estará en sitio serán presentadas al inicio del contrato. El INC se reserva el derecho de verificar la autenticidad de la información suministrada.

- REDES. El contratista deberá garantizar la disponibilidad, confiabilidad, continuidad y capacidad de la red de voz y datos a nivel físico y lógico, necesarias para su correcto funcionamiento; lo anterior incluye mantenimiento preventivo y correctivo, gestión y administración de equipos activos, administración de enlaces, canales y servicios de comunicaciones, además de instalación y traslado de puntos de red con su correspondiente certificación y maquillado.
- SEGURIDAD INFORMATICA: El contratista deberá proveer y operar de manera continua servicios administrados de seguridad informática, para mantener disponible, confiable e integra la información y la operación de todas plataformas tecnológicas, servicios conexos, y servicios administrados. Debe ejecutar la gestión continua de identificación, evaluación y corrección de vulnerabilidades y amenazas de la red, plataformas tecnológicas y servicios contratados, y garantizar la adopción de las medidas necesarias para prevenir los ataques informáticos.
- DOCUMENTACIÓN TÉCNICA. El contratista deberá mantener permanentemente actualizada toda la documentación técnica de la totalidad de temas a cargo. Esto incluye redes, equipos, seguridad y servicios.
- CAPACITACIÓN Y CAMPAÑA DE DIVULGACIÓN. El contratista deberá capacitar a todos los usuarios internos del INC en los nuevos esquemas de trabajo y en el mejoramiento de la productividad y de seguridad de la información que se pueda obtener a través del uso adecuado de la tecnología entregada. Los planes de capacitación deberán considerar usuarios finales y equipo de ingenieros que deben interactuar con la infraestructura que se instale. Adicionalmente, se deberá suministrar el plan y el material de divulgación que garantice el acceso de los usuarios a un punto único de contacto para la gestión de incidentes.
- MESA DE AYUDA. Debe implementarse una mesa de ayuda integral que registre y solucione las solicitudes de sistemas, y que registre y trámite las de otras áreas o servicios diferentes. El trámite de las solicitudes que no son de sistemas, incluye: recibir llamada, clasificar el servicio, registrar los datos de la solicitud, enviar la solicitud al área correspondiente; luego recibe el reporte de resolución y envía reporte al solicitante del estado de trámite. Se emitirán reportes permanentes del estado de avance de las solicitudes realizadas. Para cada servicio debe emitirse un número de tiquete de servicio, el cual se le suministra al solicitante. Este número se le informa al solicitante. Además del seguimiento permanente a las solicitudes, debe ubicarse una carpeta pública que permita que el solicitante consulte el estado de avance de su solicitud. Para ello podrá implementarse un aplicativo básico.

3. CARACTERISTICAS ESPECÍFICAS DEL SERVICIO

3.1. Descripción del servicio de Outsourcing para infraestructura de tecnología informática

Bajo la modalidad de Outsourcing, el INC busca optimizar los procesos de comunicación a través de la red de datos, impresión y procesamiento, garantizando la incorporación de una infraestructura de cómputo acorde con las necesidades actuales y proyectada durante la vigencia del contrato, que esté apoyada por un óptimo y permanente servicio de soporte a usuarios finales.

El software sobre el cual se realice el control de la administración de todos los servicios y de la totalidad de la infraestructura a cargo deberá permitir el acceso, a nivel de consulta, de los supervisores del contrato designados por el Instituto, con el ánimo de realizar la supervisión y auditoría de forma permanente y en línea. No se podrán tomar decisiones que afecten los servicios, la instalación y/o la operación en general, sin previa autorización de la supervisión técnica del contrato.

Los Acuerdos de Niveles de Servicio (ANS) se formalizarán a partir de la información consignada en las definiciones específicas de este documento, además se generarán otros que serán concertados entre las partes a la firma del acta de inicio, los cuales harán parte integral del contrato, y serán de cumplimiento obligatorio. Estos ANS se definirán según las necesidades de operación y la criticidad de los servicios relacionados, garantizando en todo caso la satisfacción oportuna y efectiva del servicio solicitado.

La entidad actualizará periódicamente los requerimientos del servicio con el fin de mantener su vigencia y alineamiento con las necesidades de los mismos. Estas actualizaciones pueden generar requerimientos menores o adicionales de servicio de carácter temporal o definitivo.

En caso de que los ANS concertados se vean afectados de forma negativa, se generarán descuentos en la liquidación mensual correspondiente al mes en que se generó la afectación y por el valor de los productos, talento humano y servicios involucrados. Estos acuerdos harán parte del acta de inicio que se firme entre las partes, una vez legalizado el contrato que se derive de la presente convocatoria.

Los equipos en modalidad de administrados, podrán pasar a la modalidad de Outsourcing, una vez se defina la necesidad de migración, cambio, obsolescencia etc.

3.1.1. Servicio de Outsourcing de impresión y escaneo

3.1.1.1. Equipos de impresión y escaneo en las modalidades de Outsourcing y administrados

Se requiere contratar el servicio de doscientos cuarenta y cinco (245) equipos de impresión y escaneo, de los cuales doscientos diecisiete (217) estarán en la modalidad de Outsourcing y dieciséis (16) en la modalidad de administrados, los cuales se referencian en el documento Anexo No. 7 TecnicosInvitacionPublica_Outsourcing.xlsx, en la pestaña AnexosAdmin. Los cuáles serán ubicados en las distintas áreas funcionales del Instituto, de acuerdo con la clasificación que se detalla en la Tabla 5.

El contratista debe garantizar que la totalidad de impresoras operan en perfectas condiciones bajo el sistema de información de misión crítica SAP (drivers).

Los equipos de impresión que se entreguen en la modalidad de Outsourcing deben contar con garantía durante la vigencia del contrato.

Tabla 5: Clasificación Equipos de Impresión

EQUIPOS DE IMPRESIÓN Y ESCANEO EN LAS MODALIDADES DE OUTSOURCING Y ADMINISTRADOS	
Tipo	Cantidad
Impresoras Multifuncional Modalidad Outsourcing	140
Impresoras Multifuncional Color Modalidad Outsourcing	11
Impresoras Color Estándar Modalidad Outsourcing	5
Impresoras B/N Modalidad Outsourcing	15
Impresoras Térmicas de etiquetas Modalidad Outsourcing	33
Impresoras Industrial Zebra cortadora Modalidad Outsourcing	2
Impresoras Portables Color Modalidad Outsourcing	2
Impresoras Matriz de punto carro angosto Modalidad Outsourcing	1
Impresoras Matriz de punto carro ancho Modalidad Outsourcing	1
Impresoras Datamax Modalidad Outsourcing	3
Impresora Zebra para impresión de manillas para la identificación del paciente que está hospitalizado.	4
Equipos de escaneo con alimentador ADF, escaneo dúplex, cama plana Modalidad Outsourcing	12
Impresoras Modalidad Administrados	16
Total Equipo de Impresión→	245

La configuración de los equipos deberá responder a las necesidades y requerimientos del INC, especialmente los exigidos por el sistema de información de misión crítica SAP y herramientas de oficina para los puestos de usuario final, de manera que se garanticen óptimas condiciones de trabajo.

Adicional a las cantidades requeridas, el Instituto podrá solicitar por demanda, durante su vigencia y sin que medie modificatorio al contrato, equipos adicionales, los cuales deberán corresponder a los requerimientos mínimos o superiores equivalentes a los solicitados y se pagaran a los precios pactados en el contrato que se derive de la presente convocatoria.

3.1.1.2. Impresión Por Página

El Proveedor debe ofrecer adicional al servicio de arrendamiento de los equipos tecnológicos definidos, el servicio de impresión, teniendo en cuenta los costos por página.

El precio por página impresa incluye el suministro de: (i) Tóner e insumos, (ii) repuestos por desgaste y (iii) el soporte a fallas. Para el servicio de escáner, y servicio de scan to mail, estará incluido dentro del costo del servicio. El Proveedor debe entregar los consumibles y repuestos de los equipos de impresión originales, garantizando durante la prestación del servicio la calidad de impresión. El INC durante la ejecución del Contrato podrá solicitar al Proveedor del servicio la certificación que garantice la procedencia de los consumibles que hacen parte de la ejecución del servicio. El INC, pagará únicamente por las páginas impresas, previa verificación con la herramienta de monitoreo y administración de impresiones. El INC y el Proveedor deben acordar como se realiza el suministro y cambio de consumibles durante la ejecución del contrato.

3.1.1.3. Calidad De Impresión

El proveedor debe garantizar la calidad de las impresiones, para lo cual se establecerá un protocolo de entrega de las impresoras y cambio de suministros.

3.1.1.4. Sistema de Control de Impresión.

Se requiere centralizar la gestión de impresión en un servicio que incluya los servidores locales de impresión, y su respectivo licenciamiento, que permita el balanceo de las cargas de impresión, controlando el acceso de usuarios y órdenes de impresión. Los servidores deben contar con su respectiva contingencia. Las impresoras se deben configurar de acuerdo a la necesidad y el tráfico de impresión de cada área.

Los modelos de impresoras y todo el sistema de control de impresión ofertado deben ser 100% compatibles con el sistema de información de misión crítica SAP, para lo cual se deben programar y realizar pruebas previas que verificará el administrador de SAP del INC. El contratista se encargara de ejecutar las configuraciones y parametrizaciones requeridas para lograr la integración, comunicación, el correcto funcionamiento y calidad de las impresiones desde el sistema SAP.

El contratista debe garantizar la instalación del software licenciado con derechos de uso para el INC que permita automatizar la toma de datos de acuerdo a la utilización de los recursos de impresión y para el proceso de facturación relativa al volumen de impresión que se genere por equipo de impresión y centro de costo.

Las herramientas de software deben cumplir con los siguientes requerimientos:

- La información debe estar disponible a través de comunicación electrónica utilizando un navegador estándar de Internet, con el fin de tener disponible en tiempo real la información estadística que se requiera, para ser accedida por los supervisores técnicos del contrato.
- Tener la opción de fijar cuotas de impresión por usuario, de forma tal que si el usuario sobrepasa el cupo asignado inicialmente, el sistema genere las alertas correspondientes y los mensajes de precaución al usuario cuando se acerque al cupo asignado.
- Debe controlar el consumo de impresión, promedio mensual de 850.000 a blanco y negro y 30.000 de color.
- Suministrar un usuario y contraseña de la herramienta de control y gestión de impresiones para el supervisor del contrato.

Como mínimo se debe suministrar la siguiente información estadística del servicio de impresión:

- Total general impresiones mes, especificando copiado, digitalización.
- Total impresión por áreas funcionales, centros de costos, usuarios y equipos.
- Informes sobre el buen uso de los recursos por área y por usuario, que apoyen las campañas de cero papel, y el buen uso de los recursos del INC.

El contratista debe proveer la infraestructura necesaria para la gestión y control de manera continua del servicio de impresión, esta debe estar ubicada en el **DATACENTER** del INC; administrada y debidamente soportada incluyendo mantenimiento correctivo, preventivo, gestión de garantías y licenciamiento.

3.1.2. Servicio Equipo De Cómputo y servidores en Las Modalidades Outsourcing y Administrados

Se requiere servicio en mil doscientos setenta y cinco (1.275) equipos físicos, de acuerdo con la distribución que se detalla en la Tabla 6 y cumpliendo las especificaciones mínimas requeridas.

Los servidores deben ser administrados por personal en sitio conforme a los perfiles definidos garantizando el correcto funcionamiento de la plataforma, la actualización de parches y control antivirus, así como también el desarrollo e implementación de mejoras que propendan por sistemas seguros y estables.

Tabla 6: Distribución Equipos de Cómputo Outsourcing y Administrados

EQUIPOS FISICOS EN LAS MODALIDADES DE OUTSOURCING Y ADMINISTRADOS	
Tipo	Cantidad
Computadores Escritorio Modalidad Outsourcing	1055
Computadores Escritorio Modalidad Administrados	029
Computadores Portátiles Modalidad Outsourcing	135
Computadores Portátiles Modalidad Administrados	018
Computadores Workstation Modalidad Outsourcing	020
Servidores Modalidad Outsourcing	002
Servidores Modalidad Administrados	016
Total Equipo de Cómputo→	1275

Se deben garantizar los planes de contingencia respectivos y demás planes que aseguren su correcto funcionamiento y operación sin interrupciones. Realizar pruebas periódicas de los planes de contingencia y entregar informe respectivo con recomendaciones y planes de mejora. Las características de los equipos administrados, se referencian en el documento Anexo No. 7 TecnicosInvitacionPublica_Outsourcing.xlsx, en la pestaña AnexoAdmin.

Los equipos que se oferten deben corresponder a las especificaciones mínimas requeridas incluidas en la pestaña EMR, del documento anexo: Anexo No. 7 TecnicosInvitacionPublica_Outsourcing.xlsx.

Los equipos ofertados, deberán estar incluidos en la **Guía de mercado para computadoras de escritorio y portátiles empresariales Gartner, 2018 (Market Guide for Enterprise Desktops and Notebooks, 2018 - Gartner).**

Todos los equipos en la modalidad de Outsourcing deben ser entregados con garantía mínima por el tiempo de vigencia del contrato. El proponente debe garantizar que los equipos con los cuales ejecutará el contrato son nuevos, no re manufacturados. Además, debe garantizar, que está en capacidad de administrar la base instalada de los equipos que el Instituto Nacional de Cancerología considera debe permanecer dentro de la prestación del servicio.

El contratista debe garantizar la propiedad y adquisición legal de los equipos y licencias de uso del software.

El contratista deberá garantizar que cuenta con los niveles de soporte para Hardware y Software necesarios de alto nivel con el fabricante para garantizar la operación ante la imposibilidad técnica de resolverlos con el personal de la mesa de ayuda o de su organización.

Adicionalmente, deberá adquirir a todo costo y riesgo, una póliza de seguros que ampare los equipos contra daño físico, hurto parcial o total, dentro o fuera de las instalaciones del Instituto.

Esta póliza debe amparar los equipos en la modalidad de Outsourcing nombrados en estos términos, los equipos adicionales que se adicionen por demanda y a través de modificatorios al contrato que se derive. La verificación de las pólizas se realizará de manera progresiva con la instalación al igual que lo relacionado con el licenciamiento.

La configuración de los equipos deberá responder a las necesidades y requerimientos del Instituto, tales como el sistema de información SAP R/3, ISH, ISH-MED, HCM, xRPM-PS-GM-BW /RIS-PACS, herramientas de oficina y los adicionales que el INC defina, entre otros, para los puestos de trabajo de usuario final, de manera que se garanticen óptimas condiciones de trabajo. Se debe garantizar que no se generarán interrupciones en la prestación del servicio por cualquier incidente generado por la no compatibilidad del hardware/software frente a los requerimientos del Instituto.

Se debe garantizar agilidad en los procesos de sustitución tecnológica y calidad en la migración de la información, en cualquiera de las dependencias en las que se instalen equipos del contratista.

El contratista debe garantizar la logística de suministro, instalación e implementación de todos los equipos y servicios. Lo anterior incluirá una planeación de la instalación de equipos que no implique volúmenes grandes de almacenamiento dentro del INC, dado que no cuenta con áreas de bodegaje.

Como soporte del Acta de Inicio que se derive del contrato que avala el servicio de Outsourcing, el contratista deberá hacer entrega del cronograma de instalación de equipos, servidores, servicios y

licenciamiento propuesto el cual será avalado por el INC, para la totalidad de la infraestructura a cargo.

El contratista debe garantizar que los equipos portátiles contarán con bases ergonómicas, con ventilador para evitar el calentamiento del equipo si el usuario o salud ocupacional lo requiere. Dicha solicitud se realizará por parte de la supervisión cada vez que sea necesario.

El contratista debe garantizar que los discos duros de los equipos de cómputo, estén cifrados usando el chip TPM, y deberá encargarse de la administración de las contraseñas.

Con relación a la instalación de equipos de escritorio, el proponente debe garantizar la ubicación del equipo en condiciones ergonómicas adecuadas y cuidando la estética, especialmente la relacionada con la organización de los cables y protegidos de forma adecuada, conservando las distancias que permiten la fácil y adecuada manipulación de los equipos por parte de los usuarios.

Adicional a las cantidades requeridas, el Instituto podrá solicitar por demanda, durante su vigencia y sin que medie modificatorio al contrato, equipos adicionales, los cuales deberán corresponder a los requerimientos mínimos o superiores equivalentes a los solicitados y se pagaran a los precios pactados en el contrato que se derive de la presente convocatoria.

Reintegro de equipos tecnológicos: El INC podrá devolver una cantidad de equipos tecnológicos de máximo un 10% por tipo de equipo tecnológico, equipos de cómputo o impresión, del total del contrato, para lo cual deberá haber transcurrido el 50% de tiempo de ejecución del Contrato por tipo de equipos tecnológicos y dar aviso oportuno al Proveedor, indicando la fecha a partir de la cual devolverá los equipos.

El proponente debe garantizar que cuenta con equipos de contingencia en sitio, de forma tal que al retirar por fallo o mantenimiento un equipo del puesto de trabajo del usuario, éste debe ser reemplazado de inmediato por otro de iguales características. El Instituto sólo cancelará el servicio de equipos activos al servicio de los usuarios del INC. Si al retirar un equipo por fallo o mantenimiento, éste no se reemplaza por otro de iguales características, el valor equivalente al tiempo cesante será descontado del pago que se liquide correspondiente al mes en que el equipo se encontraba fuera de servicio.

En caso de que se presente un incidente que implique el cambio del equipo y este no se encuentre disponible en sitio, se aplicara lo referido en los ANS.

Cuando el personal en sitio deba ausentarse por permiso, incapacidad, vacaciones o descanso programado, debe ser reemplazo por una persona que cuente con el entrenamiento adecuado, del mismo perfil de la persona. Al momento de presentar este tipo de eventualidades, se deberá informar a la supervisión técnica del contrato el evento y presentar la hoja de vida de quien realizará el reemplazo.

3.1.3. Licenciamiento

El contratista deberá proveer el licenciamiento de ofimática, sistemas operativos, herramientas de virtualización, herramientas de seguridad y demás herramientas que estén a su cargo, los cuales se listan y detallan a continuación:

El proveedor deberá complementar en número de licencias adicionales para cubrir 100% de la infraestructura objeto del contrato actual, de la infraestructura que se adicione y de las prórrogas que se pudieran dar y se pagaran a los precios pactados en el contrato que se derive de la presente convocatoria.

3.1.3.1. Licenciamiento Ofimática Office 365

Para asegurar gestión, administración, centralización, disponibilidad y calidad de servicio, la entidad requiere el mejoramiento y actualización de la Plataforma de correo electrónico, suite de oficina y herramientas colaborativas, que permitan brindar mejores capacidades, con el uso de tecnologías recientes; el servicio deberá alojar las aplicaciones de mensajería y herramientas. Así mismo se requiere que esta plataforma ofrezca ventajas como disponibilidad, simplicidad, escalabilidad, sincronización y seguridad, a la que se pueda acceder desde cualquier dispositivo móvil; permitiendo que los colaboradores del INC puedan ser más productivos y puedan estar al día con los recursos

críticos de datos e información en tiempo real, lo cual permitirá aumentar la velocidad y la eficacia en la toma de decisiones.

Por lo anterior, la entidad necesita optimizar los procesos y procedimientos administrativos y en tal sentido, es necesario consolidar el licenciamiento Office 365 Pro Plus, E1 y Enterprise plan E3 (que incluye suite de ofimática Word, Excel, PowerPoint, Outlook, SharePoint, OneNote, Access y Skype Empresarial, correo corporativo, almacenamiento y uso compartido de archivos en línea.

En la siguiente tabla se presentan los requerimientos de servicios en la Nube de Office 365:

Tabla 7: Licenciamiento Total

LICENCIAMIENTO OFIMATICA	
Office 365 Enterprise E3	620
Office 365 Enterprise E1	780
Office 365 Pro Plus	176

En la fase inicial el INC utilizará el siguiente licenciamiento

Tabla 8: Licenciamiento Inicial

LICENCIAMIENTO OFIMATICA	
Office 365 Enterprise E3	620
Office 365 Enterprise E1	500
Office 365 Pro Plus	176

EL INC podrá aumentar o disminuir la cantidad de licencias de office de acuerdo a las necesidades institucionales y los pagos se liquidaran mensualmente conforme al número de licencias activas.

De acuerdo con lo descrito en esta tabla, el Oferente deberá:

- Realizar una capacitación técnica avanzada para diez (10) colaboradores designados por el INC, en la plataforma de administración desarrollada por el fabricante Microsoft.
- Facturación mensual y pago por uso, es decir, solo se pagarán en el mes las licencias activas y en uso por los usuarios.
- Actualmente el INC cuenta con 419 licencias de Microsoft office Estándar y profesional en sus versiones 2013 y 2016, las cuales deberán ser utilizadas y además complementar en número de licencias adicionales para cubrir 100% la infraestructura objeto del contrato actual y de las prórrogas que se pudieran dar.
- El costo del licenciamiento no podrá exceder los establecidos en los acuerdos marco de precios de Colombia Compra Eficiente.
- La oferta económica deberá ser presentada con valores en pesos colombianos (COP). •
- En la oferta económica, deberán quedar discriminadas y contempladas las tarifas y los valores correspondientes a los impuestos y costos a que haya lugar, correspondientes a los servicios ofertados.
- Los precios ofrecidos deberán sostenerse durante la validez de la propuesta y la ejecución del contrato y sus adicionales si hay lugar a ellos. •
- La oferta económica no deberá superar la disponibilidad presupuestal asignada para el presente proceso, so pena de rechazo.

Las versiones de Office 365 deben tener las siguientes características:

3.1.3.1.1. Office 365 Enterprise E1 incluye:

3.1.3.1.1.1. Herramientas conocidas de Office

- Office en tabletas y celulares

3.1.3.1.1.2. Servicios en línea

- Correo electrónico y calendarios – Exchange Online
- Reuniones en línea – Microsoft Teams
- Difusión de reunión -Skype for Business
- Mensajería instantánea y conectividad a Skype

3.1.3.1.1.3. Servicios complementarios

- Audio conferencia - Skype for Business
- Voz moderna con el sistema telefónico
- Multi-Geo Capabilities en Office 365

3.1.3.1.2. Office 365 Enterprise E3 incluye:

3.1.3.1.2.1. Herramientas conocidas de Office

- Conjunto de aplicaciones de Office de escritorio: Word, Excel, PowerPoint, Outlook, OneNote, Publisher, SharePoint, One Drive, Microsoft Teams, Access
- Office en equipos PC, tabletas y teléfonos

3.1.3.1.2.2. Servicios en línea

- Correo electrónico y calendarios – Exchange Online
- Correo avanzado + DLP y Legal Hold
- Control de acceso a documentos y correos - Rights Management Services
- Cifrado de mensajes
- Reuniones en línea – Microsoft Teams
- Difusión de reunión -Skype for Business
- Mensajería instantánea y conectividad -Skype for Business
- Centro para el trabajo en equipo – Microsoft Teams
- Almacenamiento y uso compartido de archivos – SharePoint Online
- Intranet y sitios de grupo – SharePoint Online
- Red social corporativa - Yammer
- Office Online
- Herramientas de administración del trabajo – Microsoft Planner
- Narraciones digitales de calidad profesional - Sway
- Movilidad
- Administración empresarial de aplicaciones
- Detección y búsqueda inteligentes – SharePoint Online
- Servicio de video empresarial - Stream
- Integración de buzón de voz (Mensajería unificada)
- Herramientas de cumplimiento avanzadas
- Protección de la información
- Inteligencia empresarial con características de autoservicio en Excel – Power Pivot
- Aplicaciones para Office y SharePoint
- Automatización de flujo de trabajo - Flow
- Desarrollo de aplicaciones para Web y dispositivos móviles – PowerApps
- Servicios complementarios
- Audio conferencia – Microsoft Teams Online Meeting
- Voz moderna con Sistema telefónico – Microsoft Teams Voice Calling
- Multi-Geo Capabilities en Office 365

3.1.3.1.3. Office 365 Pro Plus incluye:

3.1.3.1.3.1. Herramientas conocidas de Office

- Conjunto de aplicaciones de Office
- Office en equipos PC, tabletas y teléfonos

3.1.3.1.3.2. Servicios en línea

- Almacenamiento y uso compartido de archivos - OneDrive
- Office Online
- Narraciones digitales de calidad profesional = Sway
- Inteligencia empresarial con características de autoservicio en Excel – Power Pivot

3.1.3.1.4. Todos los planes de Office 365 para empresas ofrecen:

- Confiabilidad
- Seguridad
- Privacidad
- Administración

- Actualizaciones
- Integración con Active Directory
- Soporte técnico
- Microsoft FastTrack para Office 365

3.1.3.2. Licenciamiento de sistemas operativos

El contratista debe garantizar el licenciamiento del sistema operativo de los equipos de cómputo, servidores físicos y virtuales contemplando el crecimiento de la infraestructura de acuerdo a las necesidades de la institución. Este licenciamiento debe cumplir con las especificaciones mínimas incluidas en la pestaña EMR, del documento Anexo No. 7 TecnicosInvitacionPublica_Outsourcing.xlsx.

3.1.3.3. Licenciamiento de herramientas de virtualización

Los servidores que el INC solicite, deberán tener licenciado la virtualización a través VMWare de acuerdo a la necesidad que se presente y la capacidad que tenga el equipo. Lo anterior con el ánimo de conservar la misma plataforma actual de los servidores administrados y facilitar la administración.

3.1.3.4. Licenciamiento de Herramientas de Control de inventarios

El contratista debe garantizar el licenciamiento del sistema de control de inventarios que oferte. Deberá garantizar usuarios para la supervisión del contrato.

3.1.3.5. Licenciamiento de Herramientas de Gestión de mesa de ayuda

El contratista debe garantizar el licenciamiento de las herramientas de gestión de mesa de ayuda basada en ITIL, y herramienta de conexión para soporte remoto. Deberá garantizar usuarios para la supervisión del contrato.

3.1.3.6. Licenciamiento de Herramientas de monitoreo.

El Contratista debe contar con licencia para herramientas de monitoreo de la plataforma activa de red WAN, LAN, canales de internet, servicios en la nube, y servidores locales al servicio del INC, que cumpla con el siguiente dimensionamiento:

Tabla 9: Monitor Red y disponibilidad

Monitor de Red y disponibilidad	
Características:	
Numero de Sensores	5000
Numero de dispositivos	500
Sondas remotas (Para distribución de carga de supervisión	Ilimitadas
Consola Centralizada	1

Se necesita que el paquete de sensores solicitado dentro del software de monitoreo que debe implantar el contratista incluya mínimo los siguientes tipos de sensores:

- Sensores Comunes: (Cloud HTTP Cloud Ping, HTTP, Ping ,Port sensor,Port Range sensor,SNMP Traffic, sensor, SSL Certificate sensor, SSL Security Check sensor, Windows Network Card)
- Sensores variados: (DHCP, DNS,IPMI System Health ,LDAP,Ping,Ping Jitter ,Port ,Port Range, RADIUS, RDP (Remote Desktop), SNMP Trap Receiver, SNTP, Syslog Receiver,SSL Security Check, Traceroute Hop Count)
- Monitoreo de Ancho de Banda
- Servidores Web (HTTP)
- SNMP
- Windows WMI/Performance
- Linux/Unix/OS X
- Servidores Virtuales
- Servidores de correo
- Servidores de base de datos
- Almacenamiento y servidores de archivos
- Dicom y HL7
- VoIP y QoS
- Parámetros de hardware
- Servicios Cloud

- IOT

3.1.3.7. Licenciamiento de Endpoint

3.1.3.7.1. Licenciamiento de Antivirus para Endpoint

El producto de Antivirus ofertado debe estar ubicado en el cuadrante de líderes de Gartner para plataformas Endpoint Protection (EPP) 2018 y/o en el cuadrante Top Players para 2018 de Radicati Endpoint Security report; y en lo posible pueda integrarse a la solución de Data Loss Prevention (DLP) para Endpoint que sea ofertada.

El contratista deberá asumir el licenciamiento de antivirus para Endpoint para el 100% de los equipos de Outsourcing y administrados, incluidos servidores físicos y virtualizados.

Tabla 10: Distribución Equipos de Cómputo Situación Actual

Antivirus	
Características:	
Número de licencias Antivirus Endpoint	1257
Número de Licencias Antivirus Servidor	18
Consola Centralizada	1

3.1.3.7.2. Licenciamiento de Data Loss Prevention –DLP, para Endpoint

El contratista, deberá licenciar la herramienta DLP (Data Loss Prevention) para Endpoint. La solución DLP ofertada deberá poder aplicar puntos de Control para uso de datos en los siguientes dispositivos:

- USB,
- CD/DVD
- Puertos COM & LPT
- Copiado/Pegado
- Unidades removibles de disco , disquetes
- Impresoras y scanners
- Infrarrojos y dispositivos de imágenes
- Pantallas
- Módems
- Puertos PCMCIA (Opcional)

Se solicita que la solución DLP de Endpoint en lo posible sea del mismo fabricante de la solución de Antivirus ofertada. Si esto no es posible se acepta una solución DLP Endpoint de diferente fabricante, pero que se encuentre registrada en el cuadrante de líderes de Gartner Magic Quadrant for Enterprise Data Loss Prevention 2017 y/o en cuadrante de Top Players de Data Loss Prevention – Market Quadrant de Radicati Group 2018.

Tabla 11: Data Loss Prevention

DLP de Endpoint	
Características:	
Número de licencias DLP Endpoint	1257
Consola Centralizada	1

3.1.3.7.3. Licenciamiento de DLP para Office 365 versión E1

El contratista debe licenciar la herramienta DLP de Microsoft (Data Loss Prevention) para todas las cuentas de Office 365 E1. Esto con el fin de completar la solución DLP para Office 365 que ya viene integrada para las cuentas de Office 365 versión E3. El DLP ofertado debe pueda crear políticas DLP mínimo para:

- Exchange Online
- OneDrive for Business
- SharePoint Online Sites
- Office desktop programs

Tabla 12: DLP total Para licencias E1

DLP total para Office 365 E1	
Número de licencias Microsoft DLP Endpoint para E1	780

En la fase inicial el INC utilizará el siguiente licenciamiento:

Tabla 13: DLP inicial Para licencias E1

DLP inicial para Office 365 E1	
Número de licencias Microsoft DLP Endpoint para E1	500

3.1.3.8. Licenciamiento de Seguridad de Red

El contratista debe garantizar el licenciamiento o inclusión de módulos de las siguientes funcionalidades de la solución de firewall de nueva generación ofertada.

Tabla 14: Características Firewall Nueva generación

FIREWALL DE NUEVA GENERACION	
Tipo	Cantidad
Intrusión Prevention System – IPS	1
Denial of Service – DOS	1
Distributed denial of service - DDOS	1
Web Access Firewall - WAF (básico, revisión x firmas)	1
Creación de sistemas virtuales en el equipo	10
Control de Aplicaciones por firmas	1
Identificación de Usuarios	1
Protección contra virus en contenido HTML y JavaScript, software espía (spyware) y gusanos (worms)	1
Consola Sandbox (en nube)	1
Identificación de Usuarios (en integración con ldap y radius)	1
Soporte para Portal Captivo	1
Token en forma nativa para permitir autenticación de 2 factores	1
Balanceo de cargas tipo SDWAN	1
Soporte de políticas QOS y Traffic Shaping	1
Filtrado de Datos para archivos y datos predefinidos	1
Control de tráfico por geolocalización	1
VPN Gateway a Gateway	2000
VPN Cliente a Gateway	50.000
Usuarios concurrentes VPN (máximo)	500
Total de Firewall de nueva generación Licenciados en HA→	2

3.1.3.9. Licenciamiento de herramienta de compresión de Archivos

El Contratista debe licenciar en todos los equipos de cómputo, servidores físicos y virtuales, la herramienta de compresión /descompresión de archivos que soporte compresión / descompresión de archivos rar.

3.1.3.10. Licenciamiento de Servicio de protección de correo Antispam

El contratista debe garantizar el licenciamiento del servicio de protección de correo electrónico Antispam en Alta disponibilidad para un paquete de 1500 usuarios de correo electrónico. Si el servicio de protección de correo se coloca en la nube, se deben licenciar y cubrir todas las cuentas de usuario contratadas de Exchange Online de Office 356, y los crecimientos futuros durante la duración del contrato.

3.1.4. Gestión De Servidores

El contratista debe administrar los servidores en la modalidad de Outsourcing y administrados.

3.1.4.1. Servidores en Outsourcing

El contratista debe disponer de dos servidores que cumplan con las especificaciones mínimas requeridas descritas en EMR-219 del Anexo No. 7 TecnicosInvitacionPublica_Outsourcing_adenda

Estos servidores se usarán para integrar servicios que actualmente tiene el INC. Estos servidores deberán contemplar el licenciamiento de sistema operativo, herramientas de virtualización y backup.

Estos servidores deberán tener un plan de respaldo y contingencia con unos altos niveles de servicio.

Los aplicativos que el INC en conjunto con el contratista migrará están descrito en el siguiente cuadro, allí mismo están descritas las licencias que tendrá que adicionar el contratista.

Configuración Requerida		MAQUINAS FISICAS				MAQUINAS VIRTUALES				
Aplicación a Instalar	Procesador	Sistema Operativo Fisico	No. Cores	RAM	Tamaño de Disco	No. Cores	RAM	Tamaño de Disco	Licencias disponibles	Sistema Operativo Virtual
VCENTER VMWARE	SERVIDOR 1	Windows Server 2016 estándar	4	16	512 GB	8	24	550gb	No se tiene disponible y la debe adquirir el proveedor.	VMware vCenter Server
Sistema de Backup para los servidores BNTTF						2	8	300GB	suministra el INC	Red Hat Linux Server V. Release 7.3.
						2	5	200GB	suministra el INC	Red Hat Linux Server V. Release 7.3.
						4	16	300GB	suministra el INC	Red Hat Linux Server V. Release 7.3.
						4	20	270GB	suministra el INC	Windows Server 2012 de 64Bits
						4	12	210GB	suministra el INC	Red Hat Liux Server V. Release 7.3.
Servidores de SIAPINC						16	36	2TB	No se tiene disponible y la debe adquirir el proveedor.	Windows 2016 Server Estándar
		2 Licencias de Virtualizador (Se licencia por socket)				8	16	2TB	No se tiene disponible y la debe adquirir el proveedor.	Windows 2016 Server Estándar
VCENTER VMWARE	SERVIDOR 2	Windows Server 2016 estándar	4	16	512 GB	8	24	550 GB	No se tiene disponible y la debe adquirir el proveedor.	VMware vCenter Server
Servidores SIGA Para laboratorio, Radiología, Hospital Día, Medicina Nuclear y Salas de Cirugía.						20	80	1TB	suministra el INC	Ubuntu 14.04.5
Servidores - Biblioteca Base de datos						4	8	640GB	suministra el INC	Debian 8.1
Servidores Control de acceso TIS,						4	16	1TB	suministra el INC	Disponible Windows Server 2012 Standard R2
Control de Acceso BIS.						4	16	1TB	suministra el INC	Disponible Windows Server 2012 Standard R2
Servidor CA Server						2	4	10GB	suministra el INC	Debian 8.1
REDCAP						3	5	500	suministra el INC	Debian 8.1
Monitor de Disponibilidad		2 Licencias de Virtualizador (Se licencia por socket)				5	8	1TB	No se tiene disponible y la debe adquirir el proveedor.	se deja abiero para cualquier sistema operativo (windows o linux
			8	32	1 TB	90	274	10.4TB		

Servidor Solicitado										
2 Servidores		Distribución Servidor B				Distribución Servidor A	Maquinas Virtuales	Sistema Operativo		Maquinas Virtuales
2 PROCESADORES de 28 CORE	56	40				42	16			16
RAM	256GB	256GB				256GB				
DISCO DURO	16TB	16TB				16TB				

3.1.4.2. Servidores modalidad administrados

El contratista debe administrar diecisiete (17) servidores en los cuales corren los servicios que se detallan en la tabla 15. La administración de estos servidores debe incluir aplicación de parches, software antivirus, control de backup/recovery, soporte a usuarios y garantizar disponibilidad de la máquina y acceso a la información permanente por parte de los usuarios.

Tabla 15: Servidores Modalidad Administrados

SERVIDORES MODALIDAD ADMINISTRADOS	
Tipo Servicio	Cantidad
Siapinc Aplicaciones	1
Siapinc Base de datos	1
NAS	1
NNAS	1
TRAZAB (Esterilización)	2
ServerLab	1
Biobanco	3
Perifoneo	1
Perifoneo	1
ATLAS (Unidad de Análisis)	1
BI	1

Control de Acceso	2
Servidor Zimbra de Respaldo	1
TOTAL SERVIDORES ADMINISTRADOS	**17**

La descripción de los servidores administrados se referencia en el documento Anexo No. 7 TecnicosInvitacionPublica_Outsourcing.xlsx, en la pestaña AnexoAdmin.

3.1.4.3. Administración de servidores

El Contratista realizará el monitoreo, la administración, soporte y mantenimiento de los equipos servidores en la modalidad, 7x24x365, con soporte en sitio.

En caso de detectarse en horas de la noche una alarma que indique una falla de servidor o la salida de operación de algún servicio esencial como DHCP, DNS, Virtualización, entre otros, el Contratista deberá presentarse inmediatamente para la corrección de la falla, dada su modalidad 7x24x365.

El Contratista debe tener en cuenta que los servidores a los que se hace referencia tienen sistemas operativos Windows y Linux, por lo cual debe contar con el personal capacitado para los servicios y procedimientos que deban efectuarse en dichas máquinas.

La Mesa de Ayuda prestará el servicio de soporte, instalación, reinstalación del sistema operativo, con arreglo de discos si lo maneja, las aplicaciones básicas de manejo del dominio, el antivirus y los parches del sistema operativo con sus respectivos servicios, así como también los sistemas manejadores de base de datos (DBMS).

Lo relacionado con el contenido de las bases de datos, la toma de backups no críticos y la restauración de los mismos, se encuentran dentro de las responsabilidades de la mesa de ayuda.

Ante el daño de los servidores administrados, el contratista deberá restaurar la operación en los tiempos definidos en los ANS, con el sistema de respaldo y backup propuesto.

La administración de servidores incluye el apoyo permanente en la verificación de la operatividad y capacidad del servidor y sus servicios, a través de las siguientes actividades:

- Identificar los recursos y la capacidad de hardware con que cuenta el servidor.
- Verificar que el hardware cumple los requerimientos mínimos establecidos por el fabricante del software, para la versión de sistema operativo instalada
- Verificar el estado de las actualizaciones, Service pack y parches del sistema operativo con las versiones correctas que se van a instalar.
- Apagado, reinicio y encendido físico del servidor, validando el correcto cargue del sistema operativo.
- Reconocimiento y disponibilidad del hardware complementario (unidades de CD/DVD, tarjetas de red).
- Verificar la conectividad a la red de datos.
- Monitorear la capacidad instalada de procesador, memoria y disco, incluyendo arreglos.
- Monitorear el acceso correcto a los recursos compartidos.
- Monitorear los servicios que corren en el servidor, en particular los pertinentes al propósito del servidor.
- Realizar el monitoreo del visor de sucesos, logs, análisis de alarmas y mensajes de error.
- Definir y ejecutar las rutinas de afinamiento al sistema operativo.
- Verificar la aplicación de las políticas de seguridad establecidas
- Revisión y monitoreo en la administración de Directorio activo, DNS, DHCP, conexiones al dominio.
- Descargar e instalar las actualizaciones y parches del programa antivirus que se encuentre instalado en el servidor, verificando su compatibilidad y determinando la conveniencia de instalación de los mismos para no afectar la integridad del sistema o el desempeño de los aplicativos.
- Realizar las acciones correctivas cuando en las actividades anteriores se detecte una falla o una no conformidad.

Adicionalmente, el Contratista deberá contar con una herramienta en línea que notifique a través de correo electrónico o mensajes de texto al celular a los administradores de los servidores y al Contratista sobre fallas técnicas (hardware y software) y alertas que se generen.

Como parte de la administración de servidores, el Contratista seguirá las siguientes políticas y en general, todas aquellas políticas del INC que sean aplicables:

- La cuenta de invitado estará deshabilitada en todos los servidores.
- La cuenta de administrador se deshabilitará y se cambiará el nombre directamente desde la directiva del dominio.
- El usuario que administrará el dominio se creará solo para este propósito y será miembro de Admins del Dominio.
- No se permite utilizar el usuario destinado para administración del dominio para que inicie sesión sobre las estaciones de trabajo. Se considera un riesgo, ya que, de existir infección sobre la estación, dicha infección puede afectar a los servidores.
- Se define la longitud, complejidad y periodicidad de las contraseñas en los servidores de acuerdo a las políticas de perfiles roles y contraseñas del INC.
- Los inicios de sesión sobre los servidores serán realizados con un usuario de pocos privilegios y para realizar tareas administrativas hacer uso del comando *run as* o ejecutar como administrador.
- Se define un tiempo de 2 minutos para que una sesión activa sea bloqueada por un screensaver.
- No se permite la existencia de recursos compartidos de control total a todos los servidores.
- Los recursos compartidos creados en un servidor tendrán un usuario o un grupo de usuarios con sus permisos de acceso específicos.
- Se tendrá un control en el software que se instalará en los servidores, existirán sólo los componentes básicos para su funcionamiento (parches, antivirus actualizado), y por ningún motivo se instalarán herramientas ofimáticas ni aplicativos que realicen descargas, y software que no se encuentre correctamente licenciado.
- La navegación por Internet en los servidores esta denegada y sólo está permitida para actualización de parches de seguridad del sistema operativo.
- Se debe hacer uso de las herramientas administrativas que existen para Windows (Adminpak) en las estaciones de los administradores de los servidores para administración del dominio y así evitar el acceso directo al servidor.
- Salvo excepciones autorizadas por el Ingeniero responsable del recurso en INC, todos los equipos cliente deben tener direccionamiento IP mediante DHCP.

Por cada servidor, el Contratista llevará una bitácora de todas las actividades sobre éstos: Acciones realizadas, niveles de rendimiento, estado de actualización de la versión del S.O y antivirus, reportes estructurados de servicios activos e inactivos dentro del servidor, registros de alertas y rendimiento, visor de sucesos y acciones tomadas. Estas anotaciones se incorporarán como un capítulo del informe mensual que el Contratista entregará a al INC.

El contratista deberá analizar la información recogida y el informe mensual presentado con el fin de identificar problemas y generar planes de mejora concertados con los administradores de plataformas del INC.

3.1.5. Gestión de Servicios de Directorio Activo, y dominio

Los servicios de autenticación y directorio activo, deberán ser compatibles con la suite de Office 365, y deben contemplar la conectividad entre el servicio de autenticación de Azure Active Directory de Office 365.

Estos servicios se deberán instalar en servidores físicos y/o virtuales proporcionados por el contratista, que cumplan con las características y especificaciones recomendadas por Microsoft para servidores de dominio, y servicios AD, DHCP y DNS. Estos servidores deberán ser instalados de manera local en el Datacenter del INC.

El contratista debe garantizar la continuidad en la operación de estos servicios (7x24x365), por lo cual se debe implementar y tener disponible plan de contingencia por cada uno de estos servidores. En caso de fallo, el plan de contingencia debe activarse de inmediato, toda vez que estos servicios se consideran de alta criticidad. El servicio de Directorio activo debe ser instalado en modo alta disponibilidad (HA).

El plan de empalme, debe considerar la migración de la información que albergan los servidores y dispositivos en los que actualmente corren estos servicios.

La gestión de los servidores junto con el soporte preventivo, correctivo debe estar contemplada dentro de la propuesta que se presente, así como la gestión y operación por personal técnico especializado en cada una de las plataformas.

Debe prestarse soporte a las plataformas con miras al cumplimiento de las políticas internas de seguridad informática.

El proveedor está en libertad de ofertar características iguales o superiores a las recomendadas por Microsoft, o esquemas de trabajo que garanticen la mayor productividad y oportunidad que se espera de estos servicios, como por ejemplo virtualización. Igualmente se deberá incluir el licenciamiento del software operativo y software de gestión que se requiera para uso exclusivo del Instituto Nacional de Cancerología.

La contingencia para los servicios de dominio debe ser configurada de forma local.

Estos servicios deberán ser realizados en su totalidad por el personal de mesa de ayuda conforme a los perfiles solicitados.

3.1.5.1. Servicios de Directorio Activo

Las tareas de administración y operación de los servicios de directorio activo estarán a cargo del contratista y entre otras serán las siguientes:

- Gestión de cuentas de equipo, usuario y grupos: Creación, modificación y eliminación de cuentas de usuario, así como creación y gestión de grupos.
- Gestión de acceso a los recursos: Control de permisos sobre todos los recursos compartidos que se encuentran en los servidores como impresoras, carpetas, aplicativos, entre otros.
- Implementación de políticas de grupo: Creación, modificación y eliminación de políticas de grupo y dominio, controlando los niveles de acceso de los equipos del INC sobre los recursos y servicios de los servidores.
- Gestión del entorno del equipo y usuario utilizando políticas de grupo: Creación, modificación, eliminación y asignación de políticas de grupo y dominio, controlando los niveles de acceso de los equipos del INC sobre los recursos y servicios de los servidores.
- Configuración y monitoreo de los servicios asociados de red como WINS, DNS, DHCP y Directorio Activo:
- Configuración o restauración del backup de los servicios de dominio en caso de ser necesario.

3.1.5.2. Administración y operación de los servicios asociados a red

El Contratista realizará configuración y Monitoreo de los siguientes servicios asociados de red:

- Servicio DHCP
- Servicio WINS
- Servicio DNS
- Servicio Active Directory
- Servicio RADIUS (Remote Authentication Dial In User Server)

El Contratista realizará gestión de prevención y recuperación de desastres frente a los servicios anteriores, configurando los servidores alternos disponibles para el cumplimiento de las siguientes políticas:

- Los servicios de Directorio activo, DNS y DHCP deben estar instalados en servidores independientes.
- Para los servidores que tienen Active Directory, DHCP, DNS, WINS debe existir un servidor que pueda entrar en funcionamiento luego de quedar fuera de línea el servidor principal.
- Para el servidor de dominio debe existir un servidor adicional del dominio con una réplica de su catálogo global, en esquema de alta disponibilidad.
- La disponibilidad del servicio DHCP debe tener una copia periódica de la base de datos DHCP principal en el servidor adicional. El servicio DHCP en el servidor adicional estará detenido y entrará en funcionamiento en caso de quedar fuera de línea el principal.
- El servicio DNS existirá en el servidor adicional con zonas secundarias y debe estar, tanto el DNS principal como el DNS secundario, en la configuración DHCP.
- Se debe realizar una configuración de zona DNS reversa para resolver direccionamiento de IPs en nombre de dominio.

El servicio WINS no es un servicio crítico, y en caso de quedar fuera de línea puede habilitarse en el servidor adicional sin ser necesario restaurar un Backup y ser refrescado a medida que los clientes realicen consultas WINS.

3.1.5.3. Administración y operación de los servicios de actualización de Microsoft Windows WSUS.

La Administración de los servidores WSUS será una actividad que tendrá implementada el Contratista a más tardar durante el periodo de transición.

Windows Update Services (WSUS) provee actualizaciones de seguridad para los sistemas operativos Microsoft. Los administradores pueden manejar centralmente la distribución de parches a través de actualizaciones automáticas a todas las computadoras de la red corporativa. La infraestructura de WSUS permite que desde un servidor(es) central(es) se descarguen automáticamente los parches y actualizaciones para los clientes en la organización, en lugar de hacerlo del sitio web Microsoft Windows Update. Esto ahorra ancho de banda, tiempo y espacio de almacenamiento debido a que los computadores no necesitan conectarse individualmente a servidores externos a la organización, sino que se conectan a servidores locales. El Contratista configurará y gestionará por lo menos un servidor central que provea actualizaciones WSUS de los sistemas operativos Microsoft para los servidores y computadores del INC, que será ubicado dentro del Datacenter del INC.

Si bien las descargas de actualizaciones a los servidores deben ser automáticas, la aplicación de dichas actualizaciones no debe serlo, ya que el Contratista debe efectuar las validaciones correspondientes de que la actualización a implementar no interfiera en la seguridad, y funcionamiento de los aplicativos y bases de datos alojados en dichos servidores. Esta verificación no podrá tomar más de 3 días hábiles.

De igual manera, el Contratista descargará e instalará los SP (Service Pack) y parches del sistema operativo y parches asociados a los diferentes aplicativos que se encuentran instalados en el servidor, verificando su compatibilidad y determinando la conveniencia de instalación de los mismos para no afectar la integridad del sistema o el desempeño de los aplicativos.

3.1.6. Gestión de Servicios de redes de voz, datos y conectividad.

El Contratista administrará y gestionará los servicios de red de voz y datos, además de la conectividad a internet, por medio de la infraestructura WLAN, LAN y MAN activa y pasiva en las sedes del INC.

En tal sentido, debe atender y solucionar los casos relacionados con los equipos activos de red y con la infraestructura de cableado estructurado en cada una de las sedes. Sin embargo, su responsabilidad más importante es evitar que estos casos se presenten.

El contratista debe garantizar disponibilidad de Red LAN y Wireless, Administración y mantenimiento de cableado estructurado, Movimiento de Equipos de red, Instalación de Puntos de Red Certificados CAT 6A, Suministro y Mantenimiento de UPS por centro de cableado. Administración de red para equipos Biomédicos y de IOT.

Para tal efecto la gestión de los servicios de redes del INC, deberá incluir:

3.1.6.1. Administración VLANS

El contratista administrará y gestionara la segmentación de las redes VLAN que defina el INC, en sus equipos activos y pasivos. El tráfico debe ser correctamente segmentado y se debe mantener documentada la configuración y permisos de VLANS.

3.1.6.2. Direccionamiento IP

El contratista será el encargado de la administración del direccionamiento IP, del INC, teniendo especial énfasis en la transición de IPV4 a IPV6. Dado que el Instituto para el segundo semestre de 2019, implementara un proyecto que tendrá como misión la transición a IPv6, para cumplir con la Resolución 2710 de 2017 del Ministerio de Tecnologías de la Información y las Telecomunicaciones – Min Tic, y la normatividad que la modifique o sustituya. El contratista seleccionado, deberá participar de la transición, prestando su apoyo a las actividades relacionadas con dicho proyecto.

3.1.6.3. Administración y Configuración de equipos activos.

El contratista debe administrar la red física y lógica de voz y datos del INC (alámbrica e inalámbrica) garantizando la calidad y continuidad en la operación de doscientos tres (203) equipos, de los cuales ciento siete (107) son inalámbricos y 96 alámbricos, según clasificación presentada en la **Tabla 16**.

El INC cuenta actualmente con un proveedor de telefonía el cual administra la red de voz del instituto, así mismo, el INC, se encuentra en el desarrollo de un proyecto de implementación de la adopción del protocolo IPV6 en la institución, dicho proyecto incluye la reposición de equipos activos, el rediseño, optimización y unificación de la red de cableado estructurado de voz y datos. Se estima que habrá una reducción de los centros de cableado y de los equipos activos actuales, por lo tanto, la red de voz del instituto se integrara en una única red que deberá ser administrada por el futuro contratista. El pago de los equipos activos administrados se hará inicialmente con los que se encuentre en operación al momento de la firma del contrato, y posteriormente se liquidará con los que queden finalmente producto de la reingeniería de red resultante del proyecto de red e IPV6.

El contratista deberá apoyarse en una herramienta de software que permita verificar el estado actual de los equipos activos de red, y la identificación y medición de tráfico de red.

Los equipos que se entreguen en la modalidad de Outsourcing deben contar con garantía durante la vigencia del contrato directamente del fabricante.

Tabla 16: Clasificación Equipos de Comunicaciones

EQUIPOS DE COMUNICACIONES EN LAS MODALIDADES DE OUTSOURCING Y ADMINISTRADOS	
Tipo	Cantidad
Equipos Red Alámbrica Modalidad Administrados	96
Equipos Red Inalámbrica Modalidad Administrados	107
Total Equipos de Comunicaciones →	203

3.1.6.4. Diseño y optimización lógico de redes.

El INC entregará al contratista los documentos de la situación actual de la red de voz y datos, así como su topología, diseño de conectividad y arquitectura de seguridad. Es de responsabilidad del contratista el mantener actualizado y optimizada dicha documentación.

3.1.6.5. Servicio de soporte de RED y resolución de problemas

A través de la mesa de ayuda se brindara soporte técnico a los usuarios finales y sedes del INC, en los temas relativos a la red de voz y datos, y a la conectividad del INC. Así mismo brindara soporte sobre los equipos de red alámbrica e inalámbrica del Instituto, ya sean propiedad de la entidad o contratados a terceros, cuando la entidad lo requiera.

3.1.6.6. Administración Red LAN Alámbrica

El Contratista será responsable de la administración física y lógica de las redes LAN, labor que incluye:

- Levantamiento o actualización de la configuración física y lógica de la red en documentos, diagramas y planos, de acuerdo con las recomendaciones ANSI/EIA/TIA 606.
- Configuración de los equipos activos de red.
- Monitoreo y análisis de tráfico, a través de herramientas que permitan la visualización del funcionamiento de la red LAN y WLAN en tiempo real.
- Revisión, análisis y gestión de logs, alarmas, traps, eventos, etc., incluyendo la solución de las causas de errores y advertencias registradas.
- Escalamiento, coordinación y seguimiento de actividades con proveedores de servicios de telecomunicaciones y relacionados.
- Administración del direccionamiento TCP/IP (IP privadas) y de los segmentos de red.
- Administración de las VLAN en los equipos activos de red.
- Administración y operación de las WLAN, e integración con la LAN.
- Autenticación e integración con RADIUS en los servidores de dominio.
- Integración con DHCP y Directorio Activo.
- Formulación de mejoras para optimizar la utilización de los segmentos de red y de la arquitectura lógica LAN en general.
- Las demás acciones que permitan minimizar la latencia de las redes WLAN y LAN, y reducir la ocurrencia de incidentes, requerimientos y problemas relacionados.

El Instituto entregará en custodia al contratista para su administración la totalidad de los centros de cableado con sus equipos correspondientes, los cuales estarán bajo su responsabilidad mientras se encuentre en ejecución el contrato que se derive de la presente convocatoria. Al iniciar el contrato, el contratista deberá asegurar la apertura de los centros de cableado con algún mecanismo de seguridad que garantice que sólo accederá personal autorizado a su cargo, y debe garantizar que exista trazabilidad de los ingresos y salida de los mismos. Durante el periodo de empalme, el contratista saliente hará entrega al contratista entrante del inventario detallado avalado por los supervisores técnicos designados por el INC.

3.1.6.6.1. **Suministro y Mantenimiento de UPS por Centro de Cableado.**
Como plan de contingencia eléctrico, el proponente deberá disponer de una UPS para 37 centros de cableado principales. El Instituto cuenta con treinta y ocho (38) centros y sub-centros de cableado en los diferentes edificios con la cantidad de equipos que se muestran en la **Tabla 17**. Las UPS solicitadas son utilizadas únicamente para soportar los equipos activos de los 38 centros de cableado con excepción del centro de cableado internos a la data center, donde se tienen una UPS dedicada, para toda clase e de quipos por lo cual se requieren 37 ups para centros de cableado.

Tabla 17: Centros de cableado

CENTROS DE CABLEADO		
Tipo	Cantidad	Ubicación
CC 3-2 Consulta Externa	6	Edificio Consulta Externa
CC 16 Portería Oriental	1	Edificio Administrativo
CC 3-5 Consulta Externa Piso 5	1	Edificio Consulta Externa
CC14 Correspondencia	1	Salida Calle Primera
CC 2-1-2 Imágenes Diagnosticas	4	Edificio Hospitales
CC 13 Bunker	1	Zona de Parqueadero
CC 2-2-4 Radioterapia	2	Edificio Hospitales
CC 2-1-1 Ascensor	1	Edificio Hospitales - 1 piso
CC9 Braquiterapia	2	Edificio Hospitales
CC 2-5-2 UCI	5	Edificio Hospitales
CC 2-4-2 Hematología	2	Edificio Hospitales
CC2-3-1 Tórax	2	Edificio Hospitales
CC1 Genética	1	Edificio Administrativo
CC1-2 Biología del cáncer	1	Edificio Administrativo
CC2-2-3 Cabeza y cuello	1	Edificio Hospitales
CC4 Admin Piso 2	3	Edificio Administrativo
CC17 Ciclotrón	4	Edificio Medicina Nuclear
CC 2-4-1 Yodoterapia	2	Edificio Hospitales
CC 2-5-1 Salas de cirugía	3	Edificio Hospitales
CC12 Ingeniería Hospitalaria	1	Edificio Medicina Nuclear
CC6 Morgue	3	Edificio Medicina Nuclear
CC 2-2-2 Patología	1	Edificio Medicina Nuclear
CC7 Biblioteca	1	Edificio Administrativo
CC11 Física Medica	1	Edificio Hospitales
CC8-1 Comunicaciones	1	Edificio Administrativo
CC8-2 Glosas	1	Edificio Administrativo
CC8 TAC	2	Edificio Hospitales
CC2-7-1 Hospital Día	1	Edificio Hospitales
CC2-2-1 Lab Clínico	3	Edificio Hospitales
CC 7-1 Audiovisuales	1	Edificio Administrativo
CC 2-6-1 Esterilización	2	Edificio Hospitales
CC 2-6-2 Pediatría Hospitales	2	Edificio Hospitales
CC5-2 Armado de cuentas	1	Edificio Administrativo
CC5 Admin Piso 3	5	Edificio Administrativo
CC5-1 Investigación Epide	2	Edificio Administrativo
CC1 San Juan de Dios	1	Carrera 10 # 1-59 Sur
CC0 Datacenter	10	Sistemas
CC1-3 Nuevo Gaica	2	Edificio Consulta Externa
Cantidad total de Centros de cableado 38	84	

3.1.6.6.2. **Movimiento de Equipos Activos de red**

El contratista será responsable por el movimiento y traslado de equipos activos de red si el INC así lo requiere, sin costo adicional para el Instituto.

3.1.6.6.3. **Instalación y traslado de Puntos de Red Certificados CAT 6A**

El contratista deberá encargarse de la instalación y traslado de puntos de red certificados categoría 6A, según el Instituto lo requiera.

3.1.6.6.4. **Administración equipos Activos LAN alámbrica**

La red alámbrica incluye la administración de noventa y seis (96) equipos en la modalidad administrados. La **Tabla 18**, detalla los equipos de comunicaciones alámbricas en la modalidad de administrados, todos estos son propiedad del INC. El contratista tendrá bajo su responsabilidad el control de inventario y hojas de vida por cada uno de los equipos, así como la gestión de las garantías correspondientes.

Tabla 18: Clasificación Equipos Comunicaciones Alámbricas Administrados

EQUIPOS DE COMUNICACIONES ALÁMBRICAS EN LA MODALIDAD DE ADMINISTRADOS	
Tipo	Cantidad
Switch HP-V1910	2
Switch HP-A5120	2
Switch HP-A5500	3
Switch HP-5800	2
Switch 3Com-5500G	6
Switch 3Com-4228G	4
Switch 3Com-3300XM	1
Switch 3Com-4900	1
Switch 3Com-4500G	4
Switch 3Com-4210G	7
Switch 3Com-4200G	54
Switch 3Com-4226T	2
Switch 3Com VARIOS	2
Switch Aruba 2530 24G PoE	3
Switch HP 1902s	2
Switch PLANET G5 5220-24 PL4XR	1
Total Equipos Comunicaciones Alámbricas Administrados →	96

La administración de la red alámbrica incluye el soporte a cada uno de los equipos y la gestión de las siguientes actividades:

- Actualización permanente del inventario de equipos activos
- Administración del Core y la red de datos
- Autenticación por Mac de los equipos en la red
- Gráficos del mapeo de la red
- Administración y mejoramiento del sistema de monitoreo de la red para registro automático de alertas y fallas sobre problemas.
- Instalación y administración de UPS en todos los centros de cableado con sistema de monitoreo por cableado estructurado.
- Configuración de switches cumpliendo las políticas de seguridad informática y diseño de segmentación de VLANs.
- El grupo de trabajo en sitio debe contar con equipos especializados para revisión de los puntos de datos y eléctricos.
- Monitoreo preventivo permanente.
- Documentación técnica de la red permanentemente actualizada.
- Instalación y certificación de puntos de cableado a solicitud según cantidades contratadas.

El Contratista será responsable de la administración de la infraestructura de cableado estructurado en cada sede, labor que incluye las siguientes actividades:

- Administrar, operar y gestionar la infraestructura pasiva de cableado estructurado (centros de cableado, Patch panel, distribuidores, salidas en el área de trabajo, cableado de UTP, fibra óptica y demás componentes del sistema).

- Levantamiento y actualización de diagramas y planos, de acuerdo con las recomendaciones ANSI/EIA/TIA 606.
- Marcado y documentación de los puertos de los elementos activos, puertos de los Patch panel y puertos en el área de trabajo, y la correspondencia entre ellos.
- Mantenimiento de los puntos de datos de las redes LAN, y de las tomas eléctricas reguladas.
- Mantenimiento de los cuartos de equipos y racks incluyendo la organización y peinado de racks.
- Relación de las actividades en una bitácora por cada ubicación y centro de datos, en donde se registre las distintas acciones desarrolladas, detallando hora, actividad y personal que realice dichas acciones, incluidas las actividades en los centros de cableado.
- Las demás que permitan minimizar la latencia de las redes LAN, y reducir la ocurrencia de incidentes, requerimientos y problemas relacionados, incluyendo aquellos derivados de una mala administración de los puntos del cableado.

Adicionalmente, durante el proceso de instalación, por cada equipo que se conecte a la red alámbrica se debe asignar un patch cord certificado categoría 6a, de longitud variable según la necesidad, suministrado por el proveedor.

3.1.6.7. Administración Red LAN Inalámbrica

El proponente debe garantizar el correcto funcionamiento de la señal inalámbrica en las áreas comunes internas en cada uno de seis (6) pisos, consultorios y puntos de atención al público del edificio de consulta externa; los siete (7) pisos del edificio hospitalario, incluidas las áreas de atención al público, consulta, hospitalarias, centrales de enfermería; y los tres (3) pisos del edificio administrativo. Aplicando las mejores prácticas y optimizando la infraestructura actual.

La red inalámbrica incluye la administración de ciento siete (107) equipos, los cuales veinticinco (25) estarán en modalidad de Outsourcing y ochenta y dos (82) en la modalidad de administrados. La **Tabla 19** detalla la clasificación de los equipos de comunicaciones inalámbricas.

Tabla 19: Clasificación Equipos de Comunicaciones Inalámbricas

EQUIPOS DE COMUNICACIONES INALÁMBRICAS EN LAS MODALIDADES DE OUTSOURCING Y ADMINISTRADOS	
Tipo	Cantidad
Access Point ARUBA Con Power Injector Tipo 1 Modalidad Administrados	80
Access Point ARUBA Con Power Injector Tipo 2 – APIN0315 Modalidad Outsourcing	25
Access Point HP Con Power Injector Tipo 3 Modalidad Administrados	1
Controladora ARUBA Modelo 7205 Modalidad Administrados	1
Total Equipos de Comunicaciones Inalámbricas →	107

3.1.6.8. Administración de NAC

El contratista deberá encargarse de la administración del sistema de control de acceso a red (NAC), una vez sea implementado en el INC.

3.1.6.9. Administración Conectividad Internet

Actualmente el INC cuenta con un servicio de internet, que consta de dos canales de 256 Mb y 128 Mb, además de un canal punto a punto dedicado de 20 Mb para comunicación con la sede CEPRED. El contratista deberá administrar los canales existentes.

En caso de presentarse cambios en la infraestructura descrita (por ejemplo, cambio de datacenter, cambio de operadores del INC, crecimiento de canales), el Contratista deberá asumir la administración de los canales en las condiciones que haya contratado el INC.

Mensualmente se presentarán informes del rendimiento o saturación de estos elementos de conectividad, que formarán parte del informe de gestión mensual.

3.1.6.10. Monitoreo de Red

Desde el inicio del contrato, el Contratista debe contar con herramientas de monitoreo de la plataforma activa de red WAN, LAN, canales de internet, servicios en la nube, y servidores locales al servicio del INC.

La solución de monitoreo que el contratista deberá suministrar, instalar, configurar, poner en funcionamiento, por lo menos debe tener la siguiente funcionalidad:

- Visualización, monitoreo y control 7x24x365 del estado, rendimiento y disponibilidad de los servicios tecnológicos relacionados con los servidores físicos, servidores virtuales, y equipos activos de red de la Entidad.
- Registro, solución, escalamiento, documentación, seguimiento y control sobre los diferentes incidentes presentados, incluyendo la generación de estadísticas de los mismos.
- Disposición de herramientas que le permitan el monitoreo remoto de los servidores físicos, servidores virtuales y equipos activos de red de la entidad, y la medición de tráfico.
- Escalamiento de incidentes a los terceros responsables de la infraestructura monitoreada.
- Gestión, seguimiento, actualización y solución de los incidentes y requerimientos.
- Actualización de la base de datos de conocimiento basado en los casos atendidos.
- El contratista brindará a la Entidad un monitor de 42" mínimo, para la visualización del rendimiento de redes, servidores y herramienta de seguridad informática objeto de monitoreo.

3.1.6.11. Documentación y actualización:

El contratista deberá mantener documentado y actualizado los siguientes ítems mínimos:

- Inventario de equipos Administrados
- Diagramas con la arquitectura lógica y física de cada servicio
- Guías, Manuales, Procedimientos, Formatos.
- Matriz de Roles y Responsabilidades general.
- Levantamiento o actualización de diagramas y planos del cableado estructurado de la sede.
- Levantamiento o actualización de diagramas de los cuartos de cableado y equipos activos de red, a nivel lógico y físico.
- Levantamiento o actualización de la documentación de la configuración de los equipos activos de red, a nivel lógico y físico, incluyendo configuración de IPS, de segmentos de red, NATs, VLANs y otros relevantes.
- Diagrama de arquitectura de seguridad informática y sus cambios registrados.

Durante el primer mes del periodo de transición el Contratista documentara en la CMDB los distintos tipos de diagramas, planos y vistas de arquitectura física y lógica de las redes de datos y eléctrica regulada que se entregarán por parte del INC por cada sede. La supervisión del contrato aprobará o ajustará los diagramas, planos y vistas propuestos por el Contratista.

3.1.7. Gestión de Seguridad Informática

Se requiere disponer de un esquema de protección de redes Internas a través de una arquitectura de Segmentación Interna, Seguridad tipo DLP, NAC, Seguridad Criptográfica, Antispam Avanzado Basado en firmas, y herramientas de analítica que permitan la identificación y tratamiento de eventos y amenazas de seguridad informática.

El proveedor dentro de sus actividades debe implementar dicho esquema y debe garantizar la seguridad informática y de comunicaciones de la plataforma tecnológica, a través de la adquisición, actualización y mantenimiento del hardware, software, licencias y dispositivos de seguridad de red, seguridad Endpoint, Seguridad Criptográfica, Seguridad avanzada de Email, seguridad para plataforma Office 365 y solución de analítica de eventos y amenazas, que permitan proteger de manera adecuada la infraestructura tecnológica y la información del INC. Es prioritario el continuo funcionamiento de los sistemas de información, bases de datos, servidores, equipos de usuario final, periféricos e impresoras, redes y comunicaciones, y demás plataformas tecnológicas soportadas. En virtud de lo anterior, es indispensable contar con herramientas de seguridad actualizadas y robustas, que brinden la protección necesaria para enfrentar eficientemente los riesgos de pérdida y/o daño de información y que pueda causar detención o demora en la operación normal de su plataforma tecnológica

3.1.7.1. Appliance de Seguridad (Firewall de nueva generación /Control de aplicaciones/ IPS/ DDoS)

Se debe contar con la solución de seguridad tipo Firewall de Nueva Generación en esquema de alta disponibilidad (HA), estimando que los equipos ofertados no deben superar en promedio el 50% de consumo de recursos en un tiempo de 3 años, debido a la posibilidad de que uno de los 2 equipos tome el total de la carga del INC en caso de falla del otro.

3.1.7.1.1. Generalidades de la solución de Firewall de Nueva Generación

- Deben ser equipos tipo appliance de propósito específico, diseñados para realizar las tareas de aseguramiento de red.
- El dispositivo debe ser un equipo de arquitectura integrada de propósito específico para ofrecer un alto rendimiento y baja latencia.
- Debe permitir el balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales
- El hardware debe tener la siguiente configuración mínima:
  - Dos (2) SFP + Slots de 10 GE (Gigabit Ethernet),
  - Ocho (8) interfaces RJ45 GE (Gigabit Ethernet),
  - Ocho (8) Slots SFP GE (Gigabit Ethernet),
  - Dos (2) puertos de administración RJ45 GE (Gigabit Ethernet),
  - Dos puertos USB
  - Puerto de consola Rj45
- Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red.
- Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP).
- Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3) de forma nativa, sin afectar el rendimiento del sistema.
- Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas.
- Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo.
- En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace.
- Debe soportar la creación de sistemas virtuales en el mismo equipo, mínimo 10.
- Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales.
- La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso.
- Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos).
- El sistema FW debe estar en capacidad de identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red.

3.1.7.1.2. Creación de políticas por Firewall

- Debe soportar controles de zona de seguridad.
- Debe contar con políticas de control por puerto y protocolo.
- Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones.
- Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad.
- Firewall debe poder aplicar la inspección de control de aplicaciones y filtrado web directamente a las políticas de seguridad, en vez de usar perfil obligatoriamente.
- Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;
- Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF).

3.1.7.1.3. Control de Aplicaciones

- Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;
- Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos.
- Reconocer al menos 3.000 aplicaciones diferentes, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico.
- Debe inspeccionar el payload del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo.
- Debe detectar aplicaciones a través del análisis del comportamiento del tráfico observado, incluyendo, pero no limitado a las aplicaciones de VoIP que utilizan cifrado propietario y BitTorrent.
- Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la DeepWeb y redes TOR.
- Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante.
- Debe hacer decodificación de protocolos con el fin de detectar aplicaciones encapsuladas dentro del protocolo y validar que el tráfico corresponde a la especificación del protocolo.
- Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas.
- Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos.
- Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas.
- Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante.
- La creación de firmas personalizadas debe permitir el uso de expresiones regulares, el contexto (sesiones o transacciones), utilizando la posición en el payload de paquetes TCP y UDP, y el uso de decodificadores de al menos los siguientes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, SSL y RTSP.
- El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos.
- Debe alertar al usuario cuando sea bloqueada una aplicación.
- Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo.
- Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo.
- Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video.
- Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo.
- Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc).
- Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas.

3.1.7.1.4. Prevención de Amenazas

- Debe incluir la protección contra ataques de denegación de servicio.
- Debe tener los siguientes mecanismos de inspección IPS: Análisis de patrones de estado de las conexiones; Análisis de decodificación de protocolo; Análisis para detectar anomalías de protocolo; Análisis heurístico; Desfragmentación IP; Re ensamblado de paquetes TCP. Bloqueo de paquetes con formato incorrecto (malformed packets);

- Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc.
- Detectar y bloquear los escaneos de puertos de origen.
- Bloquear ataques realizados por gusanos (worms) conocidos.
- Contar con firmas específicas para la mitigación de ataques DoS y DDoS.
- Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow).
- Debe poder crear firmas personalizadas en la interfaz gráfica del producto.
- Debe permitir utilizar operadores de negación en la creación de firmas personalizadas de IPS o anti-spyware, permitiendo la creación de excepciones con granularidad en la configuración.
- Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3.
- Soportar el bloqueo de archivos por tipo.
- Identificar y bloquear la comunicación con redes de bots.
- Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo.
- Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación.
- Debe permitir la captura de paquetes por tipo de firma IPS y definir el número de paquetes capturados o permitir la captura del paquete que dio lugar a la alerta, así como su contexto, facilitando el análisis forense y la identificación de falsos positivos.
- Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos.
- Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms).
- Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP.
- Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad.
- Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes de seguridad, incluyendo NGFW y Sandbox (en la nube).
- Identificar anomalías en el tráfico analizado, generando acciones automáticas preventivas y de remediación en la red, mediante módulos de Indicadores de Compromiso (IOC), identificando equipos clientes comprometidos por una situación de malware, botnet o C&C.
- Realizar un análisis de los archivos en línea y aplicar una política de remoción de contenido dinámico en tiempo real, generando un archivo plano, seguro y sin componentes sospechosos para los usuarios. Esta funcionalidad debe permitir como mínimo el análisis de archivos PDF y Microsoft Office en los protocolos HTTP (GET), SMTP, IMAP y POP3.

3.1.7.1.5. Identificación de Usuarios

- Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local.
- Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios.
- Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y grupos de usuarios.

- Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo).
- Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios.
- Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD.
- Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.
- Proporcionar al menos un token de forma nativa, lo que permite la autenticación de dos factores.

3.1.7.1.6. Balanceo, traffic shaping y QoS

- Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming.
- Soportar la creación de políticas de QoS y Traffic Shaping por características como dirección de origen, dirección destino, usuarios y grupos de usuario, aplicaciones.
- En QoS debe permitir la definición de tráfico con características como ancho de banda garantizado, máximo BW y colas de prioridad.
- Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.
- Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service).
- Proporcionar estadísticas en tiempo real para clases de QoS y Traffic Shaping.
- Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes.
- Generar políticas para garantizar las mejores condiciones de acceso a redes a través de la aplicación de reglas de balanceo tipo SDWAN. Mediante este componente, se debe realizar una evaluación de condiciones entre los diferentes enlaces WAN como jitter, BW, latencia y pérdida de paquetes para determinar el mejor canal a emplear para el intercambio de información de aplicaciones críticas.

3.1.7.1.7. Filtrado de Datos

- Debe permitir la creación de filtros para archivos y datos predefinidos.
- Los archivos deben poder ser identificados por tamaño y tipo.
- Debe permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.).
- Debe soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos.
- Debe soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos.
- Debe permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares.

3.1.7.1.8. Control por Geolocalización

- Debe soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países.
- Debe permitir la visualización de los países de origen y destino en los registros de acceso.
- Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas.

3.1.7.1.9. VPN

- Soporte VPN de sitio-a-sitio y cliente-a-sitio;
- Soportar VPN IPSec;

- Soportar VPN SSL;
- Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall, Aruba (HP)
- Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;
- Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting;
- La VPN SSL debe soportar que el usuario pueda realizar la conexión a través de cliente instalado en el sistema operativo de su máquina o a través de la interfaz web;
- Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy;
- Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiMalware para el tráfico de clientes remotos conectados a la VPN SSL;
- Soportar autenticación vía ACTIVE DIRECTORY / LDAP, Secure id, certificado y base de usuarios local;
- Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;
- Deberá mantener una conexión segura con el portal durante la sesión;
- El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows, LINUX y Mac OS;

3.1.7.1.10. Desempeño de FWNG

El Firewall de nueva generación deberá cumplir con las siguientes características mínimas de desempeño ya activas y funcionales:

- Rendimiento de Firewall (Paquetes por segundo): 22 Gbps
- Latencia de Firewall: 2 µs
- Rendimiento de IPS (Throughput): 5.2 Gpps
- Rendimiento de Inspección SSL: 5.7 Gbps
- Rendimiento VPN IPSec (Throughput): 20 Gbps
- Rendimiento de NGFW: 5 Gbps
- Rendimiento de protección de amenazas: 4.7 Gbps
- Rendimiento de control de aplicaciones (Throughput):14 Gbps
- Soporte de 8.000.000 sesiones concurrentes
- Soporte de 10.000 políticas
- Soporte a 500 usuarios VPN SSL

3.1.7.1.11. Administración de Firewall de Nueva generación (FWNG)

El Contratista deberá proveer el personal calificado y prestara el servicio de soporte, instalación, actualización, configuración de reglas, configuración y administración de servicios de seguridad informática solicitados sobre el firewall de nueva generación. La administración de dicho firewall incluye el apoyo permanente en la verificación de la operatividad del appliance y sus servicios, a través de las siguientes actividades:

- Implantación, afinamiento y operación de las herramientas de seguridad Firewall de Nueva generación en esquema de alta disponibilidad (HA), incluyendo todos sus módulos y características contratadas, y de herramientas de seguridad adicionales del INC como NAC, Controladora Aruba, Software de control de Switches, Uptimerobot (disponibilidad web), herramientas de monitoreo de canales de proveedor de comunicaciones, así como las demás herramientas que el Contratista aporte para el aseguramiento de la red.
- Verificar el estado de las actualizaciones, firmware, firmas y parches liberados por el fabricante.
- Apagado, reinicio y encendido físico del firewall de nueva generación y/o módulos de seguridad, validando el correcto cargue de todos los servicios.
- Creación, mantenimiento y control de VPNs Gateway a Gateway (sitio a sitio), y VPNs Cliente a Gateway (usuario a sitio) garantizando el acceso solo a los recursos que sean requeridos o solicitados. Instalación y configuración de clientes de VPN en los equipos que lo requieran.

- Visualización, monitoreo y control 7x24x365 de la integridad, rendimiento y disponibilidad de Firewall de nueva generación. En caso de detectarse en horas de la noche, fines de semana o festivos una alarma que indique una falla de módulos/ servicios o la salida de operación de algún servicio esencial del FWNG como VPN, IPS, Balanceo de cargas, Restricciones de Navegación, DDOS, WAF entre otros, el Contratista deberá presentarse inmediatamente de forma presencial para la corrección de la falla.
- Por cada FWNG, el Contratista llevará una bitácora de todas las actividades sobre éstos: Acciones realizadas, niveles de rendimiento, estado de actualización de la versión del Firmware y firmas, reportes estructurados de servicios activos e inactivos dentro del servidor, registros de alertas y rendimiento, alertas de sucesos y acciones tomadas. Estas anotaciones se incorporarán como un capítulo del informe mensual que el Contratista entregará al INC.
- Monitorear la capacidad de procesador, memoria y disco de los Firewall en esquema HA, la cual no deben superar en promedio el 50% de consumo de recursos en un tiempo de 3 años, debido a la posibilidad de que uno de los 2 equipos tome el total de la carga del INC en caso de falla del otro.
- El Contratista deberá configurar el FWNG para realizar notificaciones a través de correo electrónico o mensajes de texto al celular a los administradores y mesa de ayuda del Contratista sobre fallas técnicas (hardware y software) y alertas que se generen.
- Monitoreo constante del funcionamiento de la infraestructura y servicios tecnológicos de INC en búsqueda de potenciales amenazas; para lo que debe usar las herramientas contratadas y las herramientas que dispone el INC y adicionalmente las que sean requeridas para ofrecer unos niveles adecuados de protección, mismos que deberá aportar el Contratista.
- Revisión y tratamiento de los eventos de seguridad, alarmas registradas por las herramientas y servicios de FWNG, y potenciales amenazas.
- Identificación adecuada y oportuna de los incidentes y eventos de seguridad; el Contratista deberá analizarlos, comunicarlos, investigarlos y reportarlos oportunamente, además de contenerlos y remediarlos en coordinación con el Oficial de Seguridad de la Información del INC
- Recolección de información de eventos de seguridad, cadena de custodia y presentación de resultados se deben ejecutar de acuerdo con técnicas propias de la informática forense.
- Realizar el cumplimiento de políticas y controles de seguridad de la información, de políticas de privacidad y manejo de datos personales del INC, y las que se definan en el SGSI (Sistema de Gestión de seguridad de la información), basados en el marco de trabajo de seguridad de información.
- Realizar las acciones correctivas cuando en las actividades anteriores se detecte una falla o una no conformidad.

3.1.7.2. Servicio de Analítica de eventos y detección de amenazas de seguridad

El servicio de analítica de eventos y detección de amenazas debe permitir recopilar, analizar y correlacionar los datos de la red distribuida desde una ubicación central, analizar todo el tráfico del firewall y generar informes desde una única consola. Debe ofrece una visión crítica de las amenazas en toda la superficie de ataque y proporcionar visibilidad instantánea, conocimiento de la situación, inteligencia de amenazas en tiempo real y análisis procesables.

3.1.7.2.1. Requerimientos Generales de solución de analítica

- La solución de appliance de analítica debe ser de la misma marca del fabricante ofertada para el Firewall de nueva generación, o garantizar total compatibilidad, integración y funcionalidad con el mismo.
- La solución de appliance de analítica, debe contar con un sistema externo de Almacenamiento de LOGs, analítica y reportes, con una capacidad mínima de 4TB de almacenamiento en disco.
- Mínimo debe contar con dos interfaces RJ45 Gigabit Ethernet, o superior.
- Debe contar con una interface de administración gráfica (GUI) vía Web (HTTPS)

- Debe contar con un interface de administración vía CLI (Línea de comando), vía ssh y consola serial
- Debe permitir la definición de dominios administrativos independientes para dividir o segmentar el control de la información recibida y almacenada por dispositivo.
- Tener la posibilidad de definir administradores para la solución, de modo que pueda segmentarse la responsabilidad de los administradores por tareas operativas
- Permitir integrar dispositivos para que reporten, y establezcan comunicaciones seguras con dichos dispositivos
- Permitir asignar cuotas de espacio en disco por dispositivo o FW virtual, de modo que un solo dispositivo no consuma la totalidad del disco de la solución
- Permitir hacer búsquedas por username o dirección IP, para que toda la información almacenada de dicho username o dirección IP sea mostrada en un reporte donde pueda darse seguimiento a su actividad.

3.1.7.2.2. Generación de Reportes

- Permitir generar reportes personalizados, permitir al administrador de la solución el determinar el contenido de los reportes.
- El contenido de los reportes incluye los datos en formato tabular (tablas) y/o gráficas
- Generar reportes de: Utilización de la red (ancho de banda o conexiones), usuarios, direcciones IP y/o servicios con mayor consumo de recursos.
- Generar reportes de los ataques detectados/detenidos con mayor frecuencia en la red, por fuente y/o por destino.
- Generar reportes de las páginas y/o categorías de URL visitadas con mayor frecuencia, por fuente y/o por destino.
- Permitir generar la incidencia de virus detectados/removidos a nivel red por fuente y/o por destino.
- Permitir generar un reporte de las actividades administrativas (entradas de administradores, cambios de configuración) realizadas.
- Permitir personalizar los criterios bajo los cuales será obtenido el reporte, tales como fuentes, destinos, servicios, fechas y/o día de la semana.
- Permitir especificar el período de tiempo específico para el cual el reporte va a ser obtenido, por períodos relativos (hoy, ayer, esta semana, semana pasada, este mes, mes pasado) o bien por períodos absolutos (de la fecha día/mes/año a la fecha día/mes/año).
- Permite la calendarización de reportes.
- Permite enviar el reporte vía correo electrónico.

3.1.7.2.3. Desempeño de solución de analítica de eventos y amenazas

El equipo analizador de eventos y amenazas deberá cumplir con las siguientes características mínimas de desempeño:

- Gigabytes por día /Logs: 100, para lo que se requieren mínimo 4 TB de almacenamiento.
- Tasa de analítica sostenida (logs/sec)*: 3000
- Tasa sostenida del colector (logs/sec): 4500
- Dispositivos / VDOMs (Dominios Virtuales): 150
- Número máximo de días de análisis: 40

3.1.7.2.4. Administración de servicio de Analítica de eventos y detección de amenazas

El Contratista deberá proveer el personal calificado y prestara el servicio de soporte, instalación, actualización, configuración, administración y gestión de la solución de analítica de eventos y detección amenazas. La administración y gestión de dicho sistema incluye las siguientes actividades:

- Configurar Firewall de nueva generación para que envíe los datos que pasan por el appliance de analítica. El contratista se encargara de la integración de nuevos dispositivos al appliance de analítica en el caso de adicionarse nuevas soluciones de seguridad. El servicio de analítica de eventos debe estar en la capacidad recibir los logs a través de syslogs de otras plataformas. El Analizador debe poder almacenar logs de otras plataformas y debe permitir búsquedas vía Syslog.

- Configurar sistema de administración de alertas y generación de eventos de appliance de analítica.
- El contratista debe adecuar e integrar a solicitud del INC, todos los archivos o servidores de logs que la entidad determine para la correlación de eventos dentro del appliance de analítica.
- El contratista deberá realizar una revisión constante de las amenazas, vulnerabilidades y alertas de seguridad identificadas por la herramienta de appliance de analítica.
- El contratista deberá desplegar en la pantalla de 42" solicitada dentro de las herramientas de monitoreo, los principales dashboard de la solución de appliance de analítica.
- El Contratista monitoreará las aplicaciones para identificar posibles ataques o intrusiones, y diagnosticará si se trata de un incidente malintencionado o una falsa alarma, y sea cual fuere el caso, determinará los riesgos sobre la operación y formulará los planes de contención y remediación, en coordinación con el Oficial de Seguridad de la Información del INC.
- Resolución adecuada y oportuna de amenazas y vulnerabilidades identificadas por la herramienta de appliance de analítica; el Contratista deberá registrarlos en el sistema de mesa de ayuda, analizarlos, comunicarlos, investigarlos, documentarlos y reportarlos oportunamente, además de contenerlos y remediarlos en coordinación con el Oficial de Seguridad de la Información del INC.
- Resolución de incidentes sobre Endpoint, servidores y dispositivos en los que se detecte mediante el appliance de analítica actividad maliciosa o sospechosa, con la correspondiente recolección de información de amenazas y vulnerabilidades que se hayan materializado, asegurando cadena de custodia y presentación de resultados manteniendo una adecuada cadena de custodia.
- Configuración de informes tipo resumen automáticos dentro de la herramienta para entregar semanalmente al Oficial de seguridad de la información del INC.
- Presentación al INC de Informe mensual de detección de amenazas y vulnerabilidades, de su respectivo tratamiento, y de la gestión de la herramienta de analítica por parte del Contratista
- Verificar el estado de las actualizaciones, firmware, firmas y parches liberados por el fabricante de appliance de analítica.
- Apagado, reinicio y encendido físico del appliance de analítica, validando el correcto cargue de todos los servicios.
- Visualización, monitoreo y control 7x24x365 de la integridad, rendimiento y disponibilidad de appliance de analítica. En caso de detectarse en horas de la noche, fines de semana o festivos una alarma que indique una falla del servicio el Contratista deberá presentarse inmediatamente de forma presencial para la corrección de la falla.
- El Contratista llevará documentación actualizada y una bitácora de, sobre todas las actividades y cambios realizados en la configuración del appliance de analítica, niveles y alertas de rendimiento, la versión del Firmware, alertas de sucesos y acciones tomadas. Estas anotaciones se incorporarán como un capítulo del informe mensual que el Contratista entregará a del INC.
- El Contratista deberá configurar el appliance de analítica para realizar notificaciones a través de correo electrónico o mensajes de texto al celular a los administradores y mesa de ayuda del Contratista sobre fallas técnicas (hardware y software) y amenazas de seguridad de tipo critico que se presenten.

3.1.7.3. Servicio de Protección de Correo Electrónico

El Instituto nacional de cancerología actualmente tiene una solución de correo basada en ZIMBRA/LINUX con una solución de seguridad Antispam tipo Mail Border. Debido a la migración de la plataforma de correo a Office 365, durante la duración del contrato se requiere la migración a una solución de seguridad de Antispam en alta disponibilidad (HA) que se integre a la nueva de correo electrónico, con capacidad mínima de protección de hasta 1.500 buzones; esta solución deberá cumplir con las características técnicas que se describen a continuación:

3.1.7.3.1. Requerimientos Generales de solución Antispam

- Debe tener la capacidad de integrarse con solución de correo basado en Office 365
- Se requiere un sistema especializado de seguridad en sitio o nube que sea capaz de proteger correo electrónico (E-mail) contra SPAM, Virus, Spyware y Gusanos (Worms).
- La Disponibilidad de la solución antispam, en caso de prestarse el servicio tipo Cloud, debe ser mínimo del 99,99 %.
- Debe ser capaz de proteger correo electrónico entrante (desde Internet) y correo saliente (hacia Internet).
- Capacidad incluida de conectarse en tiempo real a una base de datos centralizada en el fabricante de la solución ofertada para descargar actualizaciones y bases de conocimiento antispam. El fabricante del hardware, software y firmas de seguridad deberá ser el mismo.
- Capacidad de soportar múltiples dominios de correo electrónico
- Posibilidad de funcionar como SMTP mail Gateway para servidores de correo electrónico existentes.
- Debe soportar por flexibilidad, modos de operación donde el dispositivo de protección antispam se encuentra en modo transparente (bridge), en modo Gateway (relay) o en modo servidor (Donde soporte cuentas locales de correo electrónico con acceso SMTP, POP3, IMAP)
- Por seguridad y eficiencia, el sistema debe ser de propósito específico basado en un sistema operativo pre-endurecido/asegurado. No se aceptan soluciones basadas en hardware genérico y/o con sistemas operativos genéricos tales como Microsoft Windows Server.
- El servicio de correo electrónico, debe ser una solución que soporte plenamente los siguientes protocolos:
  SMTP / SMTPs
  POP3 / POP3S
  IMAP /IMAPs
  WEB MAIL / HTTPS

3.1.7.3.2. Protecciones de correo electrónico

- Debe contar con Protección contra ataques de negación de servicio por Mail Bombing
- Debe poder realizar verificaciones de DNS en reversa para proveer protección tipo Anti-Spoofing.
- Posibilidad de establecer límites en la tasa de correos enviados (E-Mail rate limit)
- Posibilidad de establecer políticas por destinatario/receptor de correo electrónico por dominio, para correo entrante o correo saliente
- Capacidad de establecer perfiles (políticas) granulares de detección de SPAM y virus. Es decir, poder definir configuraciones específicas de mecanismos Antispam / Antivirus.
- Capacidad de poder hacer cuarentena de correo, y acceder esa cuarentena mediante WebMail y POP3
- Debe contar con filtraje de archivos anexos (attachments) y contenido de mensaje de correo
- Debe poder realizar inspección profunda de cabeceras de correo.
- Capacidad de realizar filtraje estadístico y análisis Bayesiano.
- Capacidad de bloquear usando listas en tiempo real de URIs y/o URLs de SPAM
- Capacidad de configurar filtraje por palabra prohibida (Banned Word)
- Posibilidad de ejecutar rastreo por análisis de imágenes para detectar SPAM
- Debe contar con la capacidad de análisis de Fotos en los correos, capacidad de analizar JPG, GIF y PNG.
- Debe permitir soporte a listas negras (blacklist) de terceros DNSBL
- Debe permitir Revisión tipo lista gris (Graylist)
- Capacidad de Revisión de IP falsificadas (Forged IP)
- Debe permitir configuración de listas negras y blancas (usuarios/IPs permitidos o negados) a nivel global por equipo y personalizado por usuario

- Las Listas Blancas deben poder configurarse con palabras para definir correos que no son SPAM.
- Debe permitir soporte a rastreo AntiMalware de archivos comprimidos y anidados
- Posibilidad de reemplazo/edición de mensajes de notificación en AntiMalware
- Capacidad de bloqueo por tipo de archivo en AntiMalware
- Soporte de SURBL Spam URI Realtime Block. para buscar enlaces de carga útil de spam en los cuerpos de los mensajes de correo electrónico entrantes para ayudar a evaluar si los mensajes no han sido solicitados
- Capacidad de realizar Análisis Heurístico basado en los puntajes de las distintas categorías, para reconocer códigos maliciosos (virus, gusanos, troyanos, etc.) que no se encuentren en las bases de datos de firmas, ya sea porque son nuevos, o por no ser muy divulgados.
- Se deben poder crear múltiples perfiles de detección de SPAM.
- Se deben poder crear múltiples perfiles de Antivirus en email.
- Se deben poder remplazar los archivos adjuntos infectados por títulos de correos indicando que se encontró un Virus.
- El correo infectado se debe poder poner en cuarentena.

3.1.7.3.3. Cifrado de Correo Electrónico

- La solución debe soportar mecanismos de Cifrado de correo electrónico y traerlas incluidas y activas para todos los buzones requeridos, basado en identidad de usuario sin la necesidad de ser licenciado por usuarios, es decir la solución debe estar en la capacidad de encriptar correos salientes desde el momento que se instala y no debe ser necesario agregar licencias para esta característica.
- No debe ser necesario instalar software o aplicativos en el cliente para poder hacer la inscripción de correo.
- La inscripción se debe hacer basado en políticas como palabras claves en el subject.

3.1.7.3.4. Conexión/administración de plataforma

- La solución debe poderse administrar vía web a través de un puerto seguro https o vía CLI por SSH.
- Los administradores podrán asignarse por dominio y deberá poder estipular de qué equipos (por dirección IP y máscara) puede el administrador conectarse.
- Contar con soporte a por lo menos dos niveles de administración: Lectura/Escritura (Read/Write) y Sólo Lectura (Read-Only)
- Contar con soporte a SNMP versión 1 / versión 2 usando MIBS estándares y MIBS privados con Traps basadas en umbrales
- Debe proveer soporte a registro (logging) de incidentes de antivirus
- Debe contar con soporte a registro (logging) de actividad antispam
- Debe contar con soporte a un servidor syslog.

3.1.7.3.5. Reportes de solución Antispam

- Capacidad para generar reportes de actividad analizando los archivos de bitácoras (logs) y presentar la información en tablas (forma tabular) y en forma gráfica.
- Capacidad para generar reportes bajo demanda o un reporte calendarizado en intervalos específicos
- Debe incluir por lo menos 100 diferentes tipos de reportes en cinco categorías distintas, para el diferente tipo de actividad registrado
- Los reportes deben poder ser generados y enviados como PDF
- La solución debe poderse integrar a la plataforma de reportes y almacenamiento de logs de seguridad del INC.

3.1.7.3.6. Desempeño de solución Antispam

Los equipos que se oferten en el servicio deberán cumplir con las siguientes características mínimas de desempeño (en mensajes por hora):

- Email routing: 306k
- Antispam: 279k

3.1.7.3.7. Administración de solución Antispam

El Contratista deberá proveer el personal calificado y prestara el servicio de soporte, instalación, integración, actualización, configuración de reglas, configuración y administración de servicios sobre la plataforma Antispam ofertada para asegurar una protección consistente contra amenazas comunes y a avanzadas de correo electrónico.

El contratista se encargara de la gestión completa de la solución de Antispam, lo cual incluye la verificación permanente de la operatividad del sistema y sus servicios, a través de las siguientes actividades:

- Implantación, configuración y operación de solución de Antispam en esquema de alta disponibilidad (HA).
- Integrar la solución Antispam a la solución Office 365
- Administrar, monitorear y dar soporte permanente sobre los comportamientos, amenazas y vulnerabilidades detectadas por la solución de Antispam.
- El contratista debe monitorear constantemente los recursos y el comportamiento de la herramienta de antispam, y afinar las reglas de correo y niveles de seguridad para evitar bloqueos, encolamientos de correos, y latencia excesiva (delay de máximo 1 minuto).
- Identificar y solucionar los relacionados con la materialización de ataques que se filtren a través de la solución antispam, registrándolos y documentándolos en el aplicativo de mesa de ayuda.
- Realizar tratamiento sobre falsos positivos y falsos negativos de correo electrónico.
- Mantener la reputación del dominio cancer.gov.co fuera de lista negras de correo electrónico spam.
- Verificar el estado de las actualizaciones, firmware, firmas y parches liberados por el fabricante.
- Apagado, reinicio y encendido físico de la solución de Antispam y/o módulos de seguridad, validando el correcto cargue de todos los servicios.
- Generar informes mensuales de la gestión y el comportamiento de la solución antispam.

3.1.7.4. Servicios de seguridad Endpoint

El Contratista deberá proveer las herramientas y servicios de seguridad complementarias para el aseguramiento de equipos de usuarios finales (Endpoints), para que durante la vigencia del contrato los usuarios puedan ejecutar sus funciones adecuadamente y de manera segura.

3.1.7.4.1. Servicio de Antivirus con consola de administración centralizada

El Contratista debe proveer el hardware (físico o VM), la consola centralizada y las licencias de Software Antivirus con la suscripción al derecho de uso de tres (3) años para ser instaladas en todos los computadores, servidores y máquinas virtuales del INC. El Contratista deberá complementar en número de licencias adicionales para cubrir 100%, en caso de que la infraestructura objeto del contrato actual crezca por solicitud del INC, y de las prórrogas que se pudieran dar.

3.1.7.4.1.1. Requerimientos Generales

El software Antivirus suministrado por el Contratista debe cumplir con las siguientes características y funcionalidades:

- El producto de Antivirus ofertado debe estar ubicado en el cuadrante de líderes de Gartner para plataformas Endpoint Protection (EPP) 2018 y/o en el cuadrante Top Players para 2018 de Radicati Endpoint Security report; y en lo posible pueda integrarse a la solución de Data Loss Prevention (DLP) para Endpoint que sea ofertada.
- Debe contar con el servicio de consola de administración centralizada (instalada en sitio) para disponer de una administración ampliable, flexible y automatizada de las directivas de seguridad a fin de que el contratista identifique monitoree y responda a los problemas de seguridad.
- Debe contar con Protección, Detección y Eliminación de Virus y antispyware basada en firmas, ofreciendo protección para plataformas Windows, Mac y Linux.
- Debe contar con Detección del malware conocido y desconocido mediante técnicas de análisis heurístico y en tiempo real

- Debe contar con protección ante ataques de Ransomware, troyanos, gusanos, adware, phising, rootkits
- La solución debe bloquear ataques de día cero que se aprovechan de las vulnerabilidades basadas en la memoria en muchas aplicaciones populares con la reducción de puntos vulnerables en la memoria.
- Debe contar con Firewall integrado para proteger los endpoints frente a las redes de bots, los ataques de denegación de servicio distribuidos (DDoS), ejecutables no fiables, las amenazas avanzadas persistentes y las conexiones peligrosas a la Web.
- Debe poseer análisis y autoprotección de correo electrónico para clientes de correo electrónico de Internet y cliente de Microsoft Outlook, que permita el Bloqueo de correos electrónicos sospechosos y peligrosos.
- Debe poder realizar revisión y limpieza de virus dentro de archivos comprimidos.
- La consola centralizada debe poder realizar excepciones y exclusiones de servicio de Antivirus para :
  - Aplicaciones
  - Aplicaciones para supervisar
  - Extensiones
  - Archivos
  - Carpetas
  - Riesgos conocidos
  - Dominios web de confianza
  - Excepciones de Protección contra intervenciones
  - Excepciones de cambio de archivo de host o DNS

3.1.7.4.1.2. Administración de servicio de Antivirus

- El Contratista deberá realizar en la instalación y configuración de las licencias en todas las estaciones de trabajo, servidores y máquinas virtuales.
- El Contratista debe crear, probar y desplegar las ubicaciones y las políticas de seguridad determinadas que se aplique por cada ubicación o grupo. En caso de no dar continuidad con la herramienta de Antivirus actual deberán realizar el proceso de migración de software y políticas, al hardware/software que dispongan para la prestación del servicio.
- El contratista entregara al INC los respectivos medios de instalación como soporte a las licencias adquiridas. El soporte de licenciamiento se deberá de entregar al Grupo área de Sistemas una vez sea validado e instalado en los equipos de cómputo del INC, y puesta en funcionamiento la consola centralizada de administración la cual será avalada por el supervisor de contrato y el oficial de seguridad de la información del INC.
- El proveedor garantizara el funcionamiento de la solución de Antivirus, de la consola centralizada, y la protección con contraseña de los agentes en los equipos de los clientes
- Se deberá garantizar continua actualización de las bases de datos de comportamientos y firmas y mantener actualizada la consola de administración centralizada a la última versión liberada, durante todo el periodo de vigencia de contrato.
- El contratista debe administrar, monitorear y dar soporte permanente sobre los comportamientos, amenazas y vulnerabilidades detectadas por el antivirus en todos los equipos, servidores y máquinas virtuales.
- El Contratista llevará documentación actualizada y registro de incidentes y control de cambios, sobre todas las actividades, acciones y modificaciones realizadas en la configuración de la consola centralizada, alertas de rendimiento, la versión del Firmware, alertas de sucesos y acciones tomadas. Estas anotaciones se incorporarán como un capítulo del informe mensual que el Contratista entregará al INC.

3.1.7.4.2. Servicios de Data Loss Prenvention - DLP

Con el fin el fin de evitar que se comparta accidentalmente información confidencial y de asegurar la información del INC, el contratista debe proveer soluciones DLP (Data Loss Prevention) a nivel de Endpoint licenciada para todas las estaciones de trabajo objeto del contrato, y DLP para Office 365.

3.1.7.4.2.1. DLP de Endpoint

La solución DLP (Hardware, software y licencimiento) para Endpoint ofertada deberá poder aplicar puntos de control para uso de datos en los siguientes dispositivos:

- USB,

- CD/DVD
- Puertos COM & LPT
- Copiado/Pegado
- Unidades removibles de disco, disquetes
- Impresoras y scanner
- Infrarrojos y dispositivos de imágenes
- Pantallas
- Módems
- Puertos PCMCIA (Opcional)

Se solicita que la solución DLP de Endpoint en lo posible sea del mismo fabricante de la solución de Antivirus ofertada. Si esto no es posible se acepta una solución DLP Endpoint de diferente fabricante, pero que se encuentre registrada en el cuadrante de líderes de Gartner Magic Quadrant for Enterprise Data Loss Prevention 2017 y/o en cuadrante de Top Players de Data Loss Prevention –Market Quadrant de Radicati Group 2018.

3.1.7.4.2.2. DLP para Microsoft Office365

Junto con el licenciamiento ofertado de OFFICE 365, el contratista deberá adicionar y mantener el licenciamiento de la herramienta Data Loss Prevention - DLP de Microsoft Office 365 para todas las cuentas ofertadas de Office 365 versión E1. Esto con el fin cubrir el 100% del licenciamiento la solución DLP para Office 365, que ya viene como un servicio integrado para las cuentas de Office 365 versión E3.

La solución DLP de Microsoft Office 365 debe poder aplicar puntos de control e identificar información confidencial en ubicaciones de:

- Exchange Online
- OneDrive for Business
- SharePoint Online Sites
- Office desktop programs

La Solución debe permitir Supervisar y proteger la información confidencial en las versiones de escritorio de Excel, PowerPoint, y Word instaladas en los equipos.

Las políticas de DLP se deben poder crear y administran en la misma consola de administración y Centro de seguridad de la solución de Office 365.

3.1.7.4.2.3. Administración de servicio de DLP para Office 365

El contratista debe realizar la implementación, pruebas, configuración, parametrización y afinamiento de las reglas en las soluciones DLP ofertadas para cumplir con las necesidades de protección ante fuga de información.

El contratista debe sensibilizar a los usuarios de INC sobre las políticas de cumplimiento y prepararlos para las reglas que se van a aplicar

El Contratista debe monitorear los informes de DLP y cualquier informe o notificación de incidentes para asegurar la información del INC contra fugas.

Generar informes de la gestión de las herramientas DLP de manera mensual, los cuales deben ser entregados al supervisor de contrato y al Oficial de seguridad de la información.

3.1.7.5. Servicios de seguridad Criptográfica CASERVER

El contratista deberá asumir la migración, la operación y la administración de máquina virtual que contiene la entidad certificadora CAServer local configurada para trabajar con el sistema de gestión documental institucional SIAPINC IV.

Para esto el contratista debe:

- Monitorear 7X24 la operación de la máquina virtual de Ca Server. De igual manera, con base en dicho monitoreo debe mantener una bitácora con el registro del estado de la plataforma, variables de capacidad, y las acciones realizadas sobre la misma.
- Realizar las actualizaciones, aplicación de parches, y aseguramiento para Sistema Operativo de VM y de aplicación CA Server

- El contratista deberá encargarse del proceso de creación/baja de usuarios, creación de certificados, solicitud de asignación de roles y carga PKI autorizada al administrador de SIAPINC IV, e instalación de certificados digitales en los puestos de trabajo.
- Soportar y resolver los problemas que se presenten con la gestión de los certificados digitales, en coordinación con el administrador de SIAPINC IV.
- Ejecutar y resguardar adecuadamente backup periódico de la configuración de la entidad certificadora.

Para esta máquina virtual se debe tener la siguiente configuración mínima:

- 2 socket virtuales, 2 cores x socket , mínimo 1,6 GHZ
- Memoria Mínima: 4 Gb
- 250 GB de disco asignado
- 1 interfaz de red

La máquina virtual debe conservar la instalación actual y las configuraciones del siguiente software:

- Sistema Operativo Linux 8 Debian | GNU
- CA Certificate Autority software (Free)

3.1.8. Herramientas de Mesa de ayuda

3.1.8.1. Herramienta de Gestión

El Proponente debe disponer de un software de gestión basado en el modelo ITIL, para el registro, asignación, escalamiento, seguimiento, documentación y cierre de consultas, solicitudes e incidentes. La herramienta de gestión debe contar con un módulo de generación de reportes para las métricas diarias, semanales, mensuales o de cualquier otra frecuencia que se requieran por parte de la entidad. La herramienta de gestión debe contar con la infraestructura necesaria y estar debidamente licenciada.

El software de gestión de incidentes deberá permitir el control de estado de evolución del caso, adicionalmente debe registrar información acerca del estado de reparación. A partir de esta información, se debe generar una base de conocimiento que permita su consulta por personal autorizado. Debe apoyar la implementación de la estrategia ITIL, y generar las bases de conocimiento, debe integrar los usuarios de Outsourcing, y el personal de TI, propio de la institución, deben tener en cuenta el licenciamiento adjunto. La herramienta de gestión debe incluir la gestión de inventarios, la cual debe poder consolidar en línea los inventarios de Hardware y Software. Y debe generar alertas configurables sobre el comportamiento de inventarios. Se debe incluir el software de conexión remota para soporte de los equipos. Se debe poder generar encuestas de satisfacción de servicio, de manera inmediata en cuanto se cierren los casos por parte de los usuarios. La herramienta debe permitir generar informes en línea para poder validar el estado del servicio en cualquier momento.

La herramienta debe contar con al menos los siguientes módulos:

1. Administración de incidentes – IM.
2. Administración de problemas – PM.
3. Administración de cambios – CHG

La herramienta o Software debe permitir la generación de al menos los siguientes reportes:

Procedimiento de atención, diagnóstico, solución de solicitudes, seguimiento y demás variables solicitadas por El INC asociadas al servicio de Arrendamiento y al soporte técnico.

Reporte mensual del software de gestión de operaciones de TI donde se relacionen las solicitudes recibidas, la gestión realizada, los tiempos de solución y la solución entregada.

Sobre la herramienta para la gestión de incidentes, el usuario final alternativamente deberá poder reportar su caso directamente desde un browser estándar de Internet, recibir confirmación de su ticket y consultar el estado de avance de su caso.

Como mínimo, cada mes el contratista debe reportar la estadística asociada y los indicadores de cumplimiento del servicio frente a requerimientos de los usuarios.

Este servicio debe cumplir como mínimo con los siguientes requerimientos:

- Realizar el seguimiento, administración y control del inventario a cargo, por medio de una herramienta de soporte informático que debe ser suministrada por el contratista, así como los equipos de cómputo, impresión y comunicaciones que se requieran para su operación.
- El proveedor deberá garantizar el sistema de comunicaciones interno de los miembros la mesa de ayuda a través de telefonía celular o sistema de radio de la manera que lo estime conveniente con el ánimo de garantizar la comunicación efectiva entre el personal y agilizar la atención de la prestación del servicio.
- Actualizar los inventarios de toda la infraestructura a cargo, a nivel de software y hardware, registrando novedades tales como solicitud de usuario, mantenimiento correctivo, mantenimiento preventivo, cambio de partes, cambio por garantía, entre otros. Cada componente de la infraestructura a cargo deberá contar con hoja de vida en la herramienta de soporte informático, a la cual deberá poder acceder en tiempo real, los supervisores técnicos que designe el Instituto.
- La herramienta deberá estar licenciada y ser totalmente compatible con ambiente Windows. El software deberá enviar la notificación de apertura y cierre del incidente, de forma automática al usuario relacionado.
- Atender todo tipo de solicitudes de soporte informático (hardware, software, redes, aplicativos de oficina), reportados por los usuarios de la entidad. El sistema de gestión de incidentes debe retornar de inmediato el número de identificación del caso (ticket) registrado al usuario, confirmándole que se ha dado inicio a la resolución del mismo. A partir de este número, el usuario deberá poder consultar la herramienta vía web para verificar el estado de avance del caso.
- El software de gestión de incidentes debe permitir el control de estado de evolución del caso, adicionalmente debe registrar información acerca del estado de reparación. A partir de esta información, se debe generar una base de conocimiento que permita su consulta por personal autorizado.
- Las personas que atiendan la línea telefónica o buzón se responderán de acuerdo a los ANS establecidos, para dar solución telefónica al problema, de no ser así, la llamada se escalará inmediatamente al Ingeniero o Técnico del contratista, para que sea atendido en sitio. Los técnicos y/o ingenieros asignados para atender las solicitudes realizadas por los usuarios deberán dar solución en los tiempos de respuesta estipulados (acuerdos de niveles de servicio).
- Se debe garantizar soporte 7x24 en sitio.
- El proveedor es responsable de la solución completa de los incidentes, para esto deberá contar los niveles de soporte necesarios para su resolución en los tiempos definidos en los ANS.
- El soporte de Tercer nivel puede ser remoto en horario no laboral o en sitio según complejidad del incidente.
- El Proveedor podrá tomar control remoto del equipo tecnológico una vez el usuario del equipo lo autorice, con el objetivo de realizar el diagnóstico de la falla reportada y dar solución a la misma, no obstante, debe dar cumplimiento a los ANS definidos.
- El servicio de mesa de ayuda se encargará del seguimiento de todas las llamadas, desde el inicio hasta la solución definitiva de los casos.

3.1.8.2. Herramienta de gestión de inventarios

La herramienta de gestión de inventario debe contar con la infraestructura necesaria y estar legalmente licenciada con derechos de uso para el Instituto Nacional de Cancerología y debe contar como mínimo con las funcionalidades que a continuación se detallan con relación al control de inventarios, distribución de software.

El software debe ser capaz de responder a la necesidad de administración que presenta para el instituto la utilización de múltiples dispositivos, los avances de la computación en la nube y las tecnologías de virtualización. Debe permitir a los usuarios utilizar las aplicaciones y dispositivos que necesitan, manteniendo el control sobre las políticas de seguridad del Instituto. Esta solución debe unificar la administración de la infraestructura a través de una herramienta que permita gestionar equipos de cómputo, dispositivos móviles y escritorios virtuales. Además, deberá consolidar la protección contra vulnerabilidades y malware, proveyendo reportes fácilmente.

Entre las características de administración que debe tener se encuentran

Control Inventarios

- **Inventario de activos de TI automatizado**

La Herramienta deberá permitir descubrir de manera inteligente y automatizada los componentes de software y de hardware que están instalados en el ecosistema de TI del Instituto. Deberá permitir la recolección y consulta en línea de inventario de software y hardware y el control de hojas de vida de la infraestructura a cargo.

- **Gestión, Consolidación y control de inventarios de licencias:**
  Deberá ofrecer un repositorio para acreditación de licencias, que puede ser comparado contra los datos suministrados por las herramientas de inventario para ofrecer a la organización una visión de dónde hay falta de licencias (so pena de auditorías de conformidad) o exceso de licencias (desperdicio de dinero en compras innecesarias de software). Las herramientas de gestión de licencias también hacen seguimiento a los términos de las licencias (también conocidos como EULA) y sus fechas de caducidad.

- **Gestión de CMDB:**
  Deberá ofrecer la administración de la Base de datos de gestión de la configuración (CMDB), la CMDB es un repositorio centralizado para registrar los activos de TI, sus configuraciones y relaciones con los demás componentes.

- **Catálogo de servicios / productos**
  Deberá ofrecer una lista maestra de los activos y recursos aprobados para su uso dentro de la organización. El catálogo deberá guardar información específica del producto, tal como su nombre, edición, versión y tipo de acuerdo de licencia, además de otros datos claves. Deberá permitir la clasificación y administración de los catálogos de Sistemas de Información y catálogo de Servicios Tecnológicos.

Distribución de software

Deberá permitir las siguientes acciones

- **Gestión de parches y versiones:**
  Deberá permitir automatizar la implementación de parches de software para garantizar que los computadores estén actualizados y cumplan con los estándares aplicables de seguridad y eficiencia.
- Desinstalación y bloqueo de software o aplicativos no autorizados
- Actualización centralizada de software
- Auditoría de instalación de software
- Bloqueo de dispositivos
- Programación de actualizaciones masivas.

Gestión de solicitudes
Deberá permitir a los usuarios hacer solicitudes de productos de software, dispositivos u otros activos usando un formulario centralizado y diseñado para captar y evaluar requisitos específicos de las licencias, así como para gestionar y hacer seguimiento a los procesos de implementación y procura.

3.1.9. Compatibilidad con IPV6.

Se requiere que los equipos sean totalmente compatibles con el protocolo IPv6. Esto incluye que los equipos cumplan por lo menos con los siguientes RFCs, según aplique por tipo de dispositivo.

Notas:

- Los RFCs que se marcan con "*" son aquellos incluidos dentro del programa IPv6 Ready.
- Si alguno de los RFCs mencionados se encuentra derogado o reemplazado por un nuevo RFC, entonces deberá cumplir con su nueva versión o RFC de reemplazo. Por favor indicar el RFC de reemplazo en el caso en que haya cambiado.

De acuerdo con el tipo de dispositivo, el proveedor deberá proporcionar los dispositivos o aplicaciones de acuerdo con las siguientes categorías de equipos y de acuerdo con si son obligatorios u opcionales.

3.1.9.1. Para Host: Clientes o servidores

Obligatorios:

- IPv6 Basic specification [RFC2460]*

- IPv6 Addressing Architecture basic [RFC4291]
- Default Address Selection[RFC3484(bis)]
- Unique Local IPv6 Unicast Addresses (ULA)[RFC4193]
- ICMPv6[RFC4443]*
- DHCPv6client [RFC3315]
- SLAAC[RFC4862]*
- Path MTU Discovery [RFC1981]*
- Neighbor Discovery [RFC4861]*
- Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213]
- IPsec-v2[RFC2401, RFC2406, RFC2402]*
- IKE versión 2 (IKEv2) [RFC4306, RFC4718]*
- ISAKMP [RFC2407, RFC2408, RFC2409]*
- “MIPv6” [RFC3775, RFC5555] and “Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture” [RFC4877]
- DNS protocol extensions for incorporating IPv6 DNS resource récords [RFC3596]
- DNS message extension mechanism[RFC2671]
- DNS message size requirements[RFC3226]

Opcionales:

- Revised ICMPv6[RFC5095]
- IPv6 Router Advertisement Options for DNS Configuration [RFC6106]
- Extended ICMP for multi-part messages [RFC4884]
- SEND [RFC3971]
- SLAAC Privacy Extensions [RFC4941]
- Stateless DHCPv6 [RFC3736]
- DS(Trafficclass) [RFC2474, RFC3140]
- Cryptographically Generated Addresses[RFC3972]
- IPsec-v3[RFC4301, RFC4303, RFC4302]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- Multicast Listener Discovery version 2 [RFC3810]
- Packetization Layer Path MTU Discovery [RFC4821]

3.1.9.2. Para switches de capa 2

Obligatorios:

- MLDv2 snooping [RFC4541]
- DHCPv6 filtering [RFC3315]: DHCPv6 messages must beblocked between subscribers and the networks on
- False DHCPv6 servers can distribute addresses
- Router Advertisement (RA) filtering [RFC4862]: RA filtering must be used in the network to block unauthorized RA messages
- Dynamic "IPv6 Neighbor solicitation/advertisement" inspection [RFC4861]: There must be an IPv6 Neighbor solicitation/advertisement inspection as in IPv4 “Dynamic ARP inspection”. The table with MAC-address and link-local and other assigned IPv6-addresses must be dynamically created by SLAAC or DHCPv6 messages.
- Neighbor Unreachability Detection [NUD,RFC4861] filtering: There must be a NUD filtering function so false NUD messages cannot be sent.
- Duplicate Address Detection [DAD, RFC4429] snooping and filtering: Only authorized addresses must be allowed as source IPv6-addresses in DAD messages from each port.

Opcionales:

- Pv6 Basic specification [RFC2460]*
- IPv6 Addressing Architecture basic [RFC4291]
- Default Address Selection [RFC3484(bis)]
- ICMPv6[RFC4443]*
- SLAAC[RFC4862]*
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]

- IPv6 Routing Header [RFC2460, Next Header value 43] filtering: IPv6 Routing Header messages must not be allowed between subscriber ports and subscriber and uplink to prevent routing loops [See also RFC 5095, Deprecation of Type 0 Routing Headers in IPv6]
- UPnPfiltering: UPnP messages must always be blocked between customer ports. There may be a possibility to filter different Ether types to allow only 0x86dd between subscriber ports. And most probably you must also permit 0x800 and 0x806 for IPv4.

3.1.9.3. Para Routers o Switches de capa 3

Obligatorios:

- IPv6Basic specification [RFC2460]*
- IPv6 Addressing Architecture basic [RFC4291]
- Default Address Selection [RFC3484(bis)]
- Unique Local IPv6 Unicast Addresses (ULA)[RFC4193]
- ICMPv6 [RFC4443]*
- SLAAC [RFC4862]*
- MLDv2 snooping [RFC4541]
- Router-Alert option [RFC2711]
- Path MTU Discovery [RFC1981]*
- Neighbor Discovery [RFC4861]*
- Classless Inter-domain routing [RFC4632]
- If Dynamic interior Gateway protocol (IGP) is requested, then RIPng [RFC2080], OSPF-v3 [RFC5340] or IS-IS [RFC5308] must be supported. The contracting authority shall specify the required protocol.
- IfOSPF-v3 is requested, the equipment must comply with "Authentication/Confidentiality for OSPF-v3 "[RFC4552]
- If BGP4 protocol is requested, the equipment must comply with RFC4271, RFC1772, RFC4760, RFC1997, RFC3392 and RFC2545
- Support for QoS [RFC2474, RFC3140]
- Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213]
- Using Ipsec to Secure IPv6-in-IPv4 tunnels [RFC4891]
- Generic Packet Tunneling and IPv6 [RFC2473]
- If 6PE is requested, the equipment must comply with "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE) "[RFC4798]
- Multicast Listener Discovery version2 [RFC3810]*
- If mobile IPv6 is requested, the equipment must comply with MIPv6 [RFC3775, RFC5555] and "MobileI Pv6 Operation With IKEv2 and the Revised Ipsec Architecture" [RFC4877]
- If MPLS functionality (for example, BGP-freecore, MPLSTE, MPLSFRR) is requested, the PE-routers and route reflectors MUST support "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE) "[RFC4798]
- If layer-3 VPN functionality is requested, the PE-routers and route reflectors MUST support "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN "[RFC4659]
- If MPLS Traffic Engineering is used incombination with IS-IS routing protocol, the equipment MUST support "M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs) "[RFC5120]

Opcionales:

- Revised ICMPv6 [RFC5095]
- IPv6 Router Advertisement Options for DNS Configuration [RFC6106]
- DHCPv6 client/server [RFC3315]*
- Extended ICMP for multi-part message s[RFC4884]
- SEND [RFC3971]
- SLAAC Privacy Extensions [RFC4941]
- Stateless DHCPv6 [RFC3736]*
- DHCPv6 PD [RFC3633]*
- Route Refresh for BGP Capabilities-4[RFC2918]
- BGP Extended Communities Attribute [RFC4360]
- (QOS),Assured Forwarding[RFC2597]
- (QOS)Expedited Forwarding[RFC3246]
- Generic Routing Encapsulation[RFC2784]
- Cryptographically Generated Addresses[RFC3972]

- ProSafe-v3[RFC4301,RFC4303,RFC4302]
- IPSec-v2[RFC2401,RFC2406,RFC2402]*
- IKEversion2(IKEv2)[RFC4306,RFC4718]*
- ISAKMP[RFC2407,RFC2408,RFC2409]
- SNMP protocol[RFC3411]
- SNMP capabilities[RFC3412,RFC3413,RFC3414]
- Mib sam SNMP for IP [RFC4293] Forwarding [RFC4292], IPsec[RFC4807] and DiffServ [RFC3289]
- DNS protocol extensions for incorporating IPv6 DNS resource récords [RFC3596]
- DNS message extensión mechanism[RFC2671]
- DNS message size Requirements[RFC3226]
- 127-bitIPv6PrefixesonInter-Router Links[RFC6164]
- Packetization Layer Path MTU Discovery[RFC4821]
- WhenIS-IS routing protocol is requested, the equipment SHOULD support"M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems(IS-ISs)"[RFC5120](this support is highly recommended)

3.1.9.4. Para equipos de seguridad de red (Firewalls, IDS, IPS, etc)

Se incluyen en esta categoría los equipos: Firewall, IDS/IPS, Firewall de Aplicación.

Obligatorios:

- IPv6 Basic specification[RFC2460](FW,IPS,APFW)*
- IPv6 Addressing Architecture basic[RFC4291](FW,IPS,APFW)
- Default Address Selection[RFC3484(bis)](FW,IPS,APFW)
- ICMPv6[RFC4443](FW,IPS,APFW)*
- SLAAC[RFC4862](FW,IPS)*
- InspectingIPv6-in-IPv4protocol-41traffic, Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213](FW,IPS)
- Router-Alert option[RFC2711](FW,IPS)
- Path MTU Discovery[RFC1981](FW,IPS,APFW)*
- Neighbor Discovery[RFC4861](FW,IPS,APFW)*
- Evenifhighlydiscouraged,iftherequestisfortheBGP4protocol,theequipmentmustcomplywithRFC4271,RFC1772,RFC4760andRFC2545(FW,IPS,APFW)
- If the request is for a Dynamic internal Gateway protocol (IGP), then the required RIPng [RFC2080], OSPF-v3 [RFC5340] or IS-IS [RFC5308]. The contracting authority shall specify the required protocol.(FW,IPS,APFW)
- If the requested OSPF-v3, the device must support "Authentication/Confidentiality for OSPFv3 "[RFC4552](FW,IPS,APFW)
- Support for QoS [RFC2474,RFC3140](FW,APFW)
- Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213](FW)
- Using Ipsec to Secure IPv6-in-IPv4 Tunnels [RFC4891](FW)

Nota: Las funcionalidades que son soportadas en IPv4 actualmente en la entidad deben ser implementadas en IPv6 de forma equivalente.

Opcionales:

- Revised ICMPv6[RFC5095]
- IPv6 Router Advertisement Options for DNS Configuration[RFC6106]
- DHCPv6client/server[RFC3315]*
- Extended ICMP for Multipart Messages[RFC4884]
- SEND[RFC3971]
- SLAAC Privacy Extensions[RFC4941]
- StatelessDHCPv6[RFC3736]*
- DHCPv6PD[RFC3633]*
- BGP Communities Attribute[RFC1997]
- BGPCapabilitiesAdvertisementWITH-4[RFC3392]
- (QOS),Assured Forwarding[RFC2597]
- (QOS)Expedited Forwarding[RFC3246]
- Unique Local IPv6 Unicast Addresses(ULA)[RFC4193]
- Cryptographically Generated Addresses[RFC3972]
- IPsec-v3[RFC4301, RFC4303,RFC4302]*

- OSPF-v3[RFC5340]
- Authentication/ConfidentialityforOSPF-v3[RFC4552]
- GenericPacketTunnelingandIPv6[RFC2473]
- IPsec-v2[RFC2401, RFC2406,RFC2402]*
- IKE version2(IKEv2)[RFC4306,RFC4718]*
- ISAKMP[RFC2407,RFC2408,RFC2409]
- SNMP protocol [RFC3411]
- SNMP capabilities[RFC3412,RFC3413,RFC3414]
- DNSprotocolextensionsforincorporatingIPv6DNSresourcerecordsINTO[RFC3596]
- DNS message extensión mechanism[RFC2671]
- DNS message size requirements[RFC3226]
- Using IPSec to SecureIPv6-in-IPv4 Tunnels[RFC4891]
- Multicast Listener Discovery version2[RFC3810]*
- MLDv2 snooping [RFC4541](wheninL2orpassthroughmode)*
- Packetization Layer Path MTU Discovery[RFC4821]

3.1.9.5. Las aplicaciones deben ser totalmente compatibles con IPv6.

Por lo tanto, cualquier aplicación debe ser capaz de:

- Ser accedida, consultada, manipulada, administrada o ajustada a través del IPv6 por cualquier tipo de servicio.
- Disponer servicios a través de IPv6
- Comunicarse con otras aplicaciones, integraciones, autenticación, o cualquier otro sistema/dispositivo a través de IPv6.

3.1.10. Gestión de operaciones TI

El servicio a contratar debe incluir los equipos que se describen en las tablas 1 y 2, el licenciamiento descrito en la tabla 3, y los servicios conexos referidos en la tabla 4, y cumpliendo las especificaciones mínimas requeridas (EMR) y los requisitos Técnicos Generales (RTG) detallados en la Tabla 22 con iguales o superiores características. En el transcurso de duración del contrato, el INC, podrá adicionar unidades de cualquier tipo de equipo, licencias que cumplan con las especificaciones técnicas mínimas, equivalentes o superiores las cuales deberán ser solicitadas por parte de la supervisión del contrato, bajo los precios acordados, conforme a las necesidades adicionales que el INC requiera. Dichas solicitudes no implicaran un modificatorio al contrato, a no ser que no se cuente con el presupuesto disponible en el mismo.

El contratista deberá instalar, migrar la información y administrar los ítems que a continuación se detallan, con calidad y oportunidad.

- Administración de toda la infraestructura incluyendo servidores y sistemas de almacenamiento, tanto en la modalidad de Outsourcing como administrada.
- Soporte en sitio 7x24: Se debe garantizar el personal necesario en sitio que garantice la operación completa, incluido fines de semana y días festivos.
- Personal Profesional y técnico en sitio: todo el personal involucrado en el servicio debe ser calificado, y contar con la experiencia mínima exigida en la actividad relacionada para la que se propone el perfil.
- Insumos: se deben proveer los insumos requeridos de forma permanente para toda la infraestructura a cargo, de forma tal que se garantice la prestación continua del servicio. Esto implicará manejar existencias de respaldo en sitio (papel, tonner, etc.).
- Administración y control del inventario a cargo: Todo el inventario a cargo deberá ser controlado y administrado a través de una herramienta de software que le permita tanto al contratista como a la supervisión del contrato por parte del INC, consultar la hoja de vida del equipo desde el inicio de su administración hasta su retiro, controlando el detalle de mantenimientos e incidencias reportadas. La herramienta de gestión debe incluir la gestión de inventarios, la cual debe poder consolidar en línea los inventarios de Hardware y Software. Y debe generar alertas configurables sobre el comportamiento de inventarios.
- Control y gestión de garantías: De acuerdo con los procedimientos establecidos por el INC, el retiro e ingreso de cualquier equipo deberá cumplir con los controles de Almacén, lo cual gestionará el Instituto a nivel de documentación, pero será el contratista quien deberá gestionar ante el fabricante las garantías que se requieran.

- Mantenimiento preventivo: Tal como se describe y detalla en el apartado 3.1.10.1. Esta labor debe quedar documentada y avalada por el usuario final. El personal encargado de esta labor deberá ser diferente al asignado a la mesa de ayuda y al servicio de soporte de base.
- Mantenimiento correctivo: Cuando se deba realizar el retiro de algún equipo por mantenimiento correctivo, éste debe ser reemplazado de inmediato por un equipo de contingencia de las mismas o superiores características, de forma tal que no se vea afectada la labor de los usuarios. Esta labor debe quedar documentada y avalada por el usuario final, tal como se describe y detalla en el apartado 3.1.10.2
- Sin excepción cada vez que un equipo sea retirado por daño, robo, avería o mantenimiento deberá ser reemplazado de forma inmediata. Lo anterior cubre toda la infraestructura a cargo del contratista.
- Informes: Entregar documentación formal de la solución de los incidentes y problemas e informes mensuales de la operación. Entregar un informe mensual de gestión de la operación. Entregar un informe mensual de gestión de seguridad informática. Entregar un informe mensual de capacidad y disponibilidad de servidores y plataformas tecnológicas. Entregar un informe mensual de gestión de cambio dentro de las plataformas administradas.
- Indicadores de gestión: mensualmente el contratista deberá reportar los indicadores que permitan evaluar: Niveles de servicio, oportunidad en la atención y resolución de incidentes. Estos indicadores deberán estar apoyados en la herramienta de administración y monitoreo, de manera que los supervisores del contrato puedan acceder a esta información.
- Requerimientos externos: El contratista deberá soportar y apoyar las actividades y requerimientos que determine Control Interno, Revisoría Fiscal, Procuraduría, Gobierno Digital, MINTIC, CSIRT, CCOC, Ministerio de Salud, Superintendencia de Industria y Comercio, y demás entidades de control, con respecto a las responsabilidades y actividades a su cargo.
- Migración de datos: El contratista deberá realizar la migración de los datos contenidos tanto en las máquinas de usuario final como en los servidores en la modalidad de Outsourcing (exceptuando música, videos no institucionales y otros que en su momento se definan).
- Copias de respaldo equipos usuario final: El contratista deberá administrar el control de copias de respaldo de la información contenida en los equipos de usuario final, en la etapa de migración, para lo cual se deberá implementar un repositorio de red para el almacenamiento correspondiente, definir y socializar el procedimiento correspondiente y tener el control detallado de la gestión de copias. La infraestructura para realizar la actividad deberá ser suministrada por el proveedor de forma temporal mientras dure la migración.
- Estrategias de backup y recovery servidores: El contratista deberá administrar las copias de respaldo de los servidores a cargo. Documentar las estrategias de backups y recovery y llevar un control detallado de la gestión de copias.
- Contar con planes de contingencia que garanticen la estabilidad de los servicios y que permitan la recuperación de estos en el menor tiempo posible.
- Realizar pruebas periódicas de los planes de contingencia y entregar informe respectivo con recomendaciones y planes de mejora.
- Administración de la infraestructura y servicio de correo electrónico: El contratista deberá garantizar el cumplimiento de los ANS definidos con el proveedor de servicios de Office 365.
- Implementación y administración de Servidor de Dominio. Implementación y administración de Servidor DHCP. Administración de VLAN`s, Direccionamiento IP, Gateway, mask, Administración y Configuración de equipos activos. Revisión periódica y optimización lógica de RED. Servicio de soporte de RED y resolución de problemas, protocolos y tablas de ruteo NAT, QoS, Configuración de servicios, inventario de Equipos activos y Centros de cableado, Mantener la documentación y actualización Topología RED, Administración Red Inalámbrica - NAC, Monitoreo de Alarmas en equipos activos, Access Points, Enlaces de datos.
- Administración VPN y canales dedicados.
- Administración de la entidad certificadora CASERVER.
- Administración Servicios Windows Y/O Linux: los servicios de Administración de Correo Electrónico (Exchange Office 365), servicios de Directorio Activo, actualización de parches de aplicaciones Microsoft WSUS, virtualización, administración servidores de aplicaciones, servicios de Backup de datacenter, administración de políticas de seguridad para Windows y Linux.
- Implementación y administración de Servidor de Radius (Remote Authentication Dial-In User Service).
- Servicios de seguridad informática: El contratista deberá administrar los servicios de seguridad informática, seguridad Endpoint, seguridad de Redes, seguridad criptográfica, seguridad Email y autenticación, analítica de eventos y amenazas; administración de firewall de nueva generación, appliance se analítica de eventos y amenazas, antispam, consola de antivirus y herramientas de

seguridad informática; y brindara apoyo a la administración de seguridad de portales y servicios WEB.

- Manejo de insumos, residuos de aparatos eléctricos y electrónicos de infraestructura a cargo: El proveedor debe garantizar que se encuentra en capacidad de realizar la disposición final de aparatos eléctricos y electrónicos que se generen a partir de la infraestructura a cargo. Con la oferta se debe presentar la certificación correspondiente. El proveedor deberá generar periódicamente los certificados de disposición final de residuos tecnológicos correspondientes.
- Calidad de los equipos tecnológicos y software: El proveedor se obliga a entregar los equipos de cómputo e impresión nuevos no re manufacturados. Para el contrato y con relación a los equipos de cómputo e impresión, y al Software entregado, ante fallas recurrentes en el hardware de los equipos de cómputo o de impresión, el equipo debera ser cambiado por uno de características iguales o superiores. En caso de presentarse alguna de estas situaciones.
- Reintegro de equipos tecnológicos: El INC podrá devolver una cantidad de equipos tecnológicos de máximo un 10% por tipo de equipo tecnológico, equipos de cómputo o impresión, del total del contrato, para lo cual deberá haber transcurrido el 50% de tiempo de ejecución del Contrato por tipo de equipos tecnológicos y dar aviso oportuno al Proveedor, indicando la fecha a partir de la cual devolverá los equipos.
- En cuanto a los equipos de cómputo y los servicios de impresión el contratista deberá seguir los lineamientos tal como se describen y detallan en el apartado 3.1.1.2, 3.1.1.3 y 3.1.1.4
- Adicionalmente, deberá adquirir a todo costo y riesgo, una póliza de seguros que ampare los equipos contra daño físico, hurto parcial o total, dentro o fuera de las instalaciones del Instituto.
- Esta póliza debe amparar los equipos en la modalidad de Outsourcing nombrados en estos términos, los equipos adicionales que se adicionen por demanda y a través de modificatorios al contrato que se derive. La verificación de las pólizas se realizará de manera progresiva con la instalación al igual que lo relacionado con el licenciamiento.
- La gestión de los servicios de: Servidores, Directorio activo y dominio, Redes de voz y datos, conectividad, seguridad informática, Administración de correo electrónico, y demás servicios conexos, deberán ser realizados en su totalidad por el personal de mesa de ayuda conforme a los perfiles solicitados.

3.1.10.1. Mantenimiento Preventivo

Este servicio se realizará directamente en las instalaciones del Instituto Nacional de Cancerología, sobre todos los equipos objeto de la presente convocatoria.

El servicio comprende el levantamiento de inventario de equipos, ubicaciones, mantenimiento interno y externo de los equipos. Diagnóstico y optimización sobre el rendimiento, pruebas de operación, verificación de instalaciones de redes de voz, datos, centros de cableado y UPS ’s cumpliendo los estándares de los fabricantes. Adicionalmente, se debe llevar un control estricto sobre el licenciamiento legalmente autorizado, tanto sobre productos instalados en la modalidad de Outsourcing como aquellos adquiridos previamente por el INC. Estas labores deberán ser realizadas por personal calificado en sitio.

Se debe garantizar el mantenimiento preventivo de toda la infraestructura a cargo, de la siguiente forma:

El Proveedor debe llevar a cabo el mantenimiento preventivo propuesto en el protocolo de mantenimiento de equipos tecnológicos definido por el proveedor, acordado y avalado por el INC. Para los Equipos de cómputo se debe realizar un mantenimiento preventivo durante los primeros doce meses de operación, y para el resto del contrato dos mantenimientos preventivos por año. Para las impresoras y escáner se establece un mantenimiento preventivo durante los primeros doce meses de operación, entre los 12 y 24 meses dos mantenimientos preventivos, y entre los 24 y 36 meses, tres (3) mantenimientos preventivos para las áreas de volúmenes alto de impresión, y dos (2) mantenimientos preventivos para las áreas de volúmenes medio y bajo. Esta labor debe quedar documentada y avalada por el usuario final. El personal encargado de esta labor deberá ser diferente al asignado a la mesa de ayuda y al servicio de soporte de base. Al concluir, se debe entregar un informe detallado de las actividades realizadas por equipo, avalado por cada uno de los usuarios finales, y un informe consolidado que refiera el inventario de licencias, software y hardware en uso.

Al realizar el mantenimiento, se deberá adherir a cada equipo intervenido una identificación que registre la fecha del mantenimiento realizado, número de serie del equipo y ubicación actual.

La programación de los mantenimientos deberá considerar un cronograma que minimice la interrupción de las tareas de los usuarios del INC.

Se debe garantizar la desinfección de los equipos de cómputo e impresión en las áreas de hospitalización definidas como de alto riesgo de contaminación bacterial, utilizando elementos especializados que permitan eliminar patógenos.

El mantenimiento preventivo debe incluir la totalidad de equipos de cómputo (escritorio, portátiles, servidores), equipos de impresión y escaneo, equipos de comunicaciones y centros de cableado, tanto en la modalidad de Outsourcing como administrados. Para el caso de servidores se debe incluir el mantenimiento predictivo.

Dentro de los cinco (5) días hábiles siguientes a la terminación del mantenimiento preventivo en cada sede, el INC podrá solicitar al Contratista la realización de un seguimiento aleatorio hasta el cinco (5%) por ciento a los elementos intervenidos en cada sede, con el fin de corroborar la correcta y normal funcionalidad de los equipos.

Las actividades y resultados de los mantenimientos preventivos deberán incorporarse a la hoja de vida de los equipos en la herramienta de gestión de la Mesa de Ayuda.

El pago del servicio de Mantenimiento preventivo se hará contra los respectivos informes de mantenimiento, previa validación y verificación de la supervisión del contrato.

3.1.10.1.1. Procedimiento para los mantenimientos preventivos

Para cada tipo de elemento objeto de mantenimiento, el Contratista debe construir un procedimiento genérico de acuerdo a los estándares de la industria, que deberá tener en cuenta las operaciones a realizar de tal forma que se logre un mantenimiento preventivo completo, exhaustivo y que verdaderamente mantenga o prolongue la vida útil de los elementos o evite el detrimento de los mismos.

Como mínimo, el mantenimiento preventivo de los equipos o infraestructura incluye la limpieza externa, comprobación de las condiciones eléctricas externas, limpieza interna, ajuste mecánico de los elementos que lo requieran, comprobación y ajuste de voltajes internos, test de diagnóstico de hardware y software, calibración y lubricación de piezas móviles, más todos los demás procedimientos establecidos en cada caso por el fabricante.

Para los equipos en garantía, el mantenimiento preventivo contempla únicamente la limpieza externa, la comprobación de las condiciones eléctricas externas y los test de diagnóstico de Hardware y Software cuando aplique.

El Contratista propondrá estos procedimientos detallados para los mantenimientos preventivos de cada tipo de elemento, así como los formatos y listas de chequeo adjuntas a la Supervisión del contrato durante el primer mes del periodo de transición, anexando además el cronograma de los mismos durante la ejecución del contrato.

De igual forma, durante este periodo construirá procedimientos de mantenimiento preventivo para cada tipo de elemento para aquellos casos en que los elementos aún cuenten con garantía del proveedor, casos en que las operaciones de mantenimiento preventivo se limitarán a limpieza externa y las pruebas diagnósticas que se puedan realizar sin anular la garantía del elemento.

Los mantenimientos preventivos deben incluir por cuenta del Contratista todos los elementos de consumo, materiales, herramientas, recursos, servicios y mano de obra necesarios para su realización.

En caso que el mantenimiento preventivo no haya sido realizado de conformidad con lo concertado con la entidad, o lo establecido por la entidad en ausencia de concertación, la entidad podrá solicitar la repetición del mantenimiento preventivo a la sede o sobre los equipos en donde se dé la disconformidad, en cuyo caso el Contratista deberá repetirlo sin costo adicional para la Entidad, hasta que la entidad avale las operaciones realizadas.

A cada equipo al que se le realice el mantenimiento preventivo, deberá adherírsele una etiqueta indicando que se le realizó mantenimiento preventivo, la fecha y el técnico que hizo el mantenimiento, entre otra información que se considere relevante.

3.1.10.2. Mantenimiento Correctivo

Este servicio se prestará cada vez que el Instituto lo requiera y comprende la reparación de los equipos entregados en las modalidades de Outsourcing y administrados, incluido el diagnóstico, trámite de garantía o gestión y suministro de repuestos, cuando el caso lo requiera.

Durante el mantenimiento correctivo que se realice al equipo, éste debe ser reemplazado por un equipo de contingencia, garantizado de esta forma que no se interrumpirá la operación normal de los usuarios y/o servicios relacionados.

Se aclara que en caso de daño por tensión eléctrica se deben reemplazar las partes que se requieran o el cambio del equipo si fuere necesario. De igual forma, ante un caso de hurto, luego de la entrega del correspondiente denuncio por parte del usuario, el equipo debe ser reemplazado de inmediato, sin que el tiempo de gestión ante la aseguradora por parte del contratista, afecte la operación normal en el Instituto. En caso de no reponer de inmediato los equipos o partes en cuestión, se aplicaran los ANS acordados.

Durante el soporte o atención de casos que se preste a los distintos elementos tecnológicos del INC, cuando la remediación de los incidentes y requerimientos requiera el mantenimiento correctivo de los equipos tecnológicos, el servicio de mesa de ayuda incluye todos los costos requeridos para la realización de dicho mantenimiento correctivo, tales como mano de obra, herramientas y elementos de consumo necesarios, transportes, y todas aquellas actividades, elementos, recursos y servicios que se requieran para la habilitación del elemento.

Tanto en el mantenimiento preventivo como en el correctivo, si la Mesa de Ayuda ocasiona la perdida de la garantía del equipo intervenido, asumirá a partir de ese momento dicha garantía.

El Mantenimiento correctivo incluye la instalación de las partes requeridas para la reparación de los equipos. En el mantenimiento correctivo el Contratista debe realizar adicionalmente los ajustes necesarios para optimizar el funcionamiento de los equipos objeto de mantenimiento.

El servicio de mantenimiento correctivo tendrá lugar desde el inicio del contrato.

El mantenimiento correctivo se debe realizar en el sitio en donde se encuentra el elemento afectado. En caso que esto no sea posible, sólo se podrá retirar el elemento cuando el Contratista deje un equipo de contingencia.

Cuando se trate de equipos de cómputo, el mantenimiento correctivo incluye la instalación o reinstalación del sistema operativo o sus parches y actualizaciones si se requiere, con el arreglo de disco si lo maneja; las aplicaciones básicas de manejo del dominio, herramientas ofimáticas, antivirus, entre otras.

3.1.10.2.1. Instalación de equipos de contingencia

En el evento en que la reparación de un equipo o parte implique su retiro del puesto de trabajo del usuario, el contratista debe garantizar que dispondrá de equipos para reponerlo de inmediato, de iguales o superiores características, durante el tiempo que dure el arreglo respectivo, garantizando de esta forma que el usuario no se vea afectado al interrumpir su operación.

Todo equipo que sea retirado de su puesto de trabajo (en las modalidades de Outsourcing y administrados), y no sea reemplazado de inmediato, será descontado de acuerdo a lo establecido dentro de los Acuerdos de Niveles de Servicio.

El contratista debe garantizar un Plan de Contingencia que como mínimo dispondrá de equipos de escritorio, portátiles, impresoras, servidores, access point, lectores, escáner, según lo especificado en la hoja ProductosContingencia del archivo Anexo No. 7 TecnicosInvitacionPublica_Outsourcing.xlsx), con el fin de reemplazar los equipos que eventualmente queden fuera de servicio, bien sea por falla o mantenimiento programado.

Para el caso de los servidores, todos los servicios deben tener contingencia, y debe contar con un plan de contingencia que garantice la disponibilidad permanente.

De igual forma, en caso de fallas de cualquiera de los equipos activos de red, el Contratista deberá garantizar el adecuado funcionamiento de la red, proporcionando provisionalmente equipos activos para el uso del INC de características iguales o superiores a aquellas de los equipos afectados, de tal forma que se garantice el normal funcionamiento de las redes del INC.

El Contratista tendrá hasta el máximo tiempo de atención para el diagnóstico, y solución de incidentes de acuerdo a los ANS acordados.

Pasado el tiempo del diagnóstico y solución, el Contratista ubicará un equipo de contingencia con características iguales o superiores a las del equipo reemplazado. Esto será aplicable también mientras se da el suministro de repuestos, si ese es el caso.

Mensualmente presentará un acta con la relación de todos los elementos de contingencia provistos (PC, Impresoras, escáner, UPS, entre otros). La supervisión podrá realizar la verificación aleatoria de la condición anterior y firmará el acta a conformidad. Esta información se consolidará mensualmente, para presentarse en el informe de gestión.

El Contratista prestará el acompañamiento al usuario en el resguardo de la información y migración de la misma al equipo de contingencia durante la instalación de éste, y de vuelta al equipo del INC cuando se retire el equipo de contingencia, si es que el cambio no es definitivo.

Una vez verificada la preservación de la información por parte del usuario final, se debe proceder con la firma del acta en donde el usuario final certifique que ha tomado copia de seguridad de la información que requiere para el cambio de equipo y que ha verificado que dicha copia contenga la información. Una vez verificado lo anterior, el Contratista deberá realizar borrado seguro de la información en el equipo retirado, informando en forma efectiva esta actividad al usuario y dejando la evidencia en el acta correspondiente.

3.1.10.3. Migración, Implementación y Administración de Office 365

El contratista deberá garantizar la implementación y administración de la solución Office 365, incluida con vital importancia la solución de correo electrónico Exchange Online.

El objetivo general del INC para Office 365 Enterprise es acelerar su transformación digital mediante servicios en la nube con el fin de integrar empleados, partners, datos y procesos para aumentar el valor para el cliente y mantener su ventaja competitiva en un mundo digital.

El INC, adoptara Microsoft Office 365 Enterprise en sus versiones E1, E3 y Pro Plus, tal como se describe en el apartado 3.1.3.1 de licenciamiento de ofimática.

El INC llevara a cabo la transición de una infraestructura de TI centralizada local a una infraestructura de nube que incorpora aplicaciones de productividad empresarial y escenarios híbridos basados en la nube.

El contratista deberá asumir la migración, implementación y administración de office 365, como un proyecto interno dentro del contrato, y como tal deberá realizar las fases de Planeación, ejecución, seguimiento, capacitación y cierre.

Para tal efecto en el proceso de implementación el Contratista deberá garantizar que se sigan los procesos de implementación básica de Microsoft Office 365 como se detalla en las buenas prácticas de implementación que sugiere el fabricante las cuales se resumen a continuación:

3.1.10.3.1. Implementación de la infraestructura básica

Es el trabajo preliminar necesario antes de implementar aplicaciones de productividad empresarial (como Microsoft Teams, Flow etc.) y que incluye escenarios como la migración a Microsoft Office 365 y la automatización de actualizaciones del cliente.

El contratista seguirá las fases siguientes para planear e implementar la infraestructura básica de Microsoft Office 365 Enterprise en el INC:

Fase 1: Verificación y optimización de Redes y canales
Fase 2: Definición de Identidad y autenticación de usuarios
Fase 3: Instalación de Office 365 Pro Plus en equipos de usuario final
Fase 4: Migración e implementación de correo Electrónico Exchange Online
Fase 5: Activación e implementación de OneDrive 1TB x usuario.
Fase 6: Aplicación de controles de seguridad y protección de la información
Fase 7: Administración de dispositivos móviles
Fase 8: Capacitación y Gestión del cambio.

Antes de terminar cada fase, necesita examinar los criterios de salida, que son un conjunto de condiciones obligatorias que necesita cumplir y de condiciones opcionales que es importante tener en cuenta. Los criterios de salida de cada fase garantizan que la infraestructura de nube y local, así

como la configuración de un extremo a otro, cumplan con los requisitos de una implementación de Microsoft Office 365 Enterprise.

3.1.10.3.1.1. Verificación y Optimización de redes

En esta fase, se deben aplicar las consideraciones clave para crear una conexión estable a los servicios en la nube de Microsoft office 365 Enterprise, de acuerdo a las recomendaciones y buenas prácticas del fabricante.

3.1.10.3.1.2. Definición de Identidad y autenticación de usuarios

Se debe establecer una infraestructura de identidades y autenticación bien planeada y ejecutada para Office 365, garantizando la seguridad y un acceso más eficaz por parte de los usuarios y dispositivos autenticados a las aplicaciones de productividad empresarial y sus datos. Esto de acuerdo a las buenas prácticas de Microsoft de sincronización de autenticación y directorio activo.

3.1.10.3.1.3. Instalación de Office 365 Pro Plus en equipos de usuario final

Microsoft Office 365 E3 incluye Office 365 Pro Plus, la versión de suscripción de Office. Como Office 2019, Office 365 Pro Plus incluye todas las aplicaciones de Office y estas se instalarán directamente en los dispositivos cliente. A diferencia de Office 2019, Office 365 Pro Plus se actualiza con nuevas características de forma regular y tiene un modelo de licencias basadas en el usuario que permite que las personas instalen Office en un máximo de 5 dispositivos. En esta fase, el contratista implementará Office 365 Pro Plus en los equipos cliente, además de instalar las 419 licencias de Office 2013 y Office 2016, que posee el INC.

3.1.10.3.1.4. Instalación de servicio de Correo Electrónico Exchange Online

Exchange Online es el servicio de nube principal para el correo electrónico y calendario que ayuda a los usuarios colaboran en formas que no requieren interacción en tiempo real. Y se implementa con el servidor de correo Outlook.

Exchange Online también cuenta con capacidades de seguridad incluyen anti-malware y filtrado contra correo no deseado para proteger los buzones de correo y capacidades de prevención de pérdida de datos que impiden que los usuarios por error enviar información confidencial a personas no autorizadas.

La implementación de Exchange Online debe seguir las fases y los pasos siguientes. Es de tener en cuenta que antes de su implementación se debe haber surtido la fase dos de Definición de Identidad y autenticación de usuarios establecida en la implementación de la infraestructura básica de Microsoft Office 365.

Fase 1: Planear

En esta fase, se debe definir las estrategias de migración de la herramienta actual de correo que tiene el INC, que es ZIMBRA, y planear la implementación de Exchange Online, además de determinar cómo va a usar la organización Exchange Online.

Paso 1: Recopilar a los miembros de su implementación de Exchange Online
Paso 2: Determinar y dar prioridad a los escenarios empresariales Exchange Online
Paso 3. Definir estrategia de migración de Zimbra a Exchange online

Fase 2: Incorporar

En esta fase, planeación de los aspectos técnicos de una implementación de Exchange Online y empezar a implementar para los grupos de usuarios seleccionados.

Requisitos previos: configuración de acceso a dispositivos y autenticación

Paso 1: Completar el planeamiento técnico
Paso 2: Ejecutar una prueba piloto de TI

Se deberá ejecutar una prueba piloto de TI con las partes interesadas de la fase 1, así como con usuarios pioneros y aficionados técnicos.

Paso 3: Implementación

Después de completar al piloto de TI, se debe llevar a cabo la implementación y despliegue de Exchange Online al interior del INC. Esta implementación incluye la migración del servicio de correo electrónico local zimbra, Debe incluir esta implantación:

- Habilitación del portal de Office 365 para los servicios de colaboración para INC para aproximadamente 1400 usuarios (620 usuarios en Plan E3, 780 usuarios E1).
- Pruebas de validación del dominio.
- Confirmación del dominio de Office 365.
- Comprobar dominios adicionales.
- Verificación y configuración del flujo de correo electrónico.
- Configuración de lista global de direcciones.
- Activar los usuarios creados.
- Instalación y configuración de ADConnect para sincronizar el Directorio Activo local con los servicios de nube de Office365.
  - ✓ Configuración de ADConnect.
- Este servidor se utiliza para la sincronización de identidades (Usuarios y Contraseñas) entre el directorio activo Microsoft de la organización y la plataforma de Office 365.
- Para el proceso de sincronización se deberá contar con una cuenta en Azure Active Directory con permisos globales (Global Admin) y en el directorio activo local una cuenta con el perfil de Administrador de compañía (Enterprise Admin).
- Migración de los datos de los buzones existentes así:
  - ✓ Piloto de migración de usuarios.
  - ✓ Pruebas de envío de correo interno y externo.
  - ✓ Migración de las cuentas activas de Zimbra Versión 8.7.0.
- Configuración de la estrategia de migración.
- Configuración de conectores (tierra-nube)
- Plan de migración.
- Migración de buzones activos incluirá correos, contactos, agendas y calendarios según estrategia definida en el plan de migración.
- Se debe entregar la documentación con los procedimientos de migración de buzones en caso de que se decida realizar una migración parcial de la totalidad de los buzones existentes.
- Verificación de las aplicaciones y dispositivos que hacen retransmisión de correo, ej. ERP SAP, entre otros; y el acompañamiento y verificación de funcionamiento en Exchange Online.
- Configuración de los dominios de correo que usaran y pruebas de validación de los dos dominios.
- Configuración del flujo de correo.
- Direccionar los registros MX hacia Exchange Online.
- Integración, verificación y pruebas de Antispam con Exchange Online Protection.
- Adecuación y verificación de la plataforma ZIMBRA a modo consulta.

Fase 3: Impulsar el valor
En esta fase, completar la implantación de Exchange Online y admitir los usuarios para que puedan obtener sus beneficios.

Paso 1: Desplegar Exchange Online para el resto de la organización
Paso 2: Medir el uso e impulsar la adopción

3.1.10.3.1.5. Activación e implementación de OneDrive 1TB x usuario.

- Activación de las licencias de OneDrive For Business para los usuarios de licencias E3 Y E1 del INC.
- Instalación y configuración del cliente de OneDrive For Business en los equipos de usuarios final del INC.

3.1.10.3.1.6. Aplicación de controles de Seguridad y protección de la información
La protección de la información es un conjunto de directivas y tecnologías que definen la forma en que se transmite, almacena y procesa la información confidencial. En la fase 6, se describen características y opciones de configuración de protección de la información de Microsoft office 365 que le permiten proteger los datos y escenarios basados en la nube. Para lo cual se seguirán los siguientes pasos:

- Definir los niveles de protección de la información y la seguridad
- Configurar la clasificación para el entorno
- Configurar y optimizar los controles de seguridad para Office 365
- Configurar la administración del acceso con privilegios para Office 365

3.1.10.3.1.7. Administración de dispositivos móviles
Se debe planear y ejecutar la administración de equipos móviles de usuario final.

3.1.10.3.1.8. Capacitación y gestión del cambio
El contratista deberá asegurarse que los usuarios estén informados sobre las nuevas características y las nuevas formas de trabajar al cambiar los equipos a Windows 10 y Office 365 Pro Plus. Se deberá aprovechar la asistencia para la adopción por parte de los usuarios con Microsoft FastTrack, los materiales de aprendizaje y las plantillas de comunicación, así como nuevas formas para supervisar la aceptación y el uso por parte de los usuarios.

El contratista será responsable de la documentación y transferencia de conocimiento a los usuarios finales del INC.

Documentación y transferencia de conocimientos
Elaboración de la documentación del proyecto:

- Documentación de la configuración final de acuerdo a los procesos normales definidos de arquitectura.
- Documentación de procedimiento de configuración de clientes Outlook.

Sesiones de Transferencia de conocimientos las cuales se planearan en duración e intensidad horaria, enfocadas en la consola de administración de Office 365, esta será disponible para 10 recursos definidos por el INC, **"se debe entregar manual de usuario"**, las sesiones se harán hasta completar los siguientes temas:

Administración de usuarios.
Restablecer contraseñas.
Administrar dominios.
Suscripciones.
Revisión de inventario de licencias.
Compra de licencias.
Actualizar información comercial y facturación.
Solicitudes de servicio técnico.
Estado de solicitudes de servicio.
Escalamiento de casos.
Revisión de conectividad.
Exchange Online Protection.
Reglas de transporte.
Creación de subdominios en caso de ser necesario.
Configuración de filtros.
Revisión del módulo de herramientas de la plataforma.
SharePoint Online.
Configuración de sitios y subsitios.
Sincronización de OneDrive Pro.
Skype for business Online.
Administración de permisos.
DLP para Office 365.
Manejo de federación.
Azure Active Directory Premium.
Uso y gestión de la plataforma de sincronización de directorios (ADConnect).
Administración y asignación de licencias para usuarios.
Personalización de los portales cautivos.
Generación de reportes de la plataforma de autenticación.

Campaña de comunicaciones:
El oferente debe acompañar al INC, en el diseño de mensajes para su divulgación de la solución tecnológica implementada, buscando transmitir un mensaje positivo y que facilite la adopción de la solución por parte de las personas.
Entrega de Material de referencia existente del proveedor.
Incluir el merchandising necesario para la gestión del cambio para el personal del INC.

Capacitación a usuario funcional de office 365:
Capacitación general de nuevas funcionalidades en Office Pro Plus. Capacitación general en herramientas Online (SharePoint Online, Outlook online, Skype for Business, Yammer, One Drive). Sesiones presenciales magistrales y Sesiones personalizadas recorriendo las áreas del INC para

planes E1 y E3. El usuario funcional corresponde a los usuarios finales del INC y sus colaboradores a los que les es asignado o hace uso de alguna forma del licenciamiento/herramientas instaladas, directa o indirectamente.

Se debe realizar capacitación a usuarios funcionales que van a interactuar con la herramienta Office 365, la capacitación será sobre funcionalidad en operación y uso de los servicios y será brindada en sesiones de entrenamiento que permita a los funcionarios aclarar aspectos y mejorar su experiencia con el uso de la tecnología implementada. Para el cumplimiento de lo anterior se requiere que el contratista provea los medios para desplegar la capacitación en cada una de las áreas. El material de capacitación deberá ser previamente avalado por el INC. El plan de capacitación de usuarios finales deberá contener al menos los siguientes ítems:

Tabla 20: Tipos de capacitación Office 365

Perfil	Temario	Tiempo Estimado
Plan E1 y E3	Capacitación General de Nuevas funcionalidades Office 365 Pro Plus. Demostración y guía práctica de acceso al portal de Office 365. **Correo electrónico**: Permite al usuario crear un correo electrónico, como recuperar un correo eliminado, configuración de firma, configuración autos-respuestas, visualización del tamaño actual, configuración de reglas, creación de carpetas. **Calendario:** Compartir calendario, cita de reuniones (con Skype for Business o sin skype for business), visualización de calendarios. **Contactos**: Creación de contactos, exportación de Gmail, Hotmail, Exchange **Yammer**; La red social corporativa de la organización, como realizar publicaciones, felicitaciones y encuestas. **OneDrive:** Es una herramienta que le proporciona un lugar en la nube para almacenar, compartir y sincronizar sus archivos de trabajo. **Skype for Business:** Skype Empresarial le permite conectarse con compañeros de trabajo o socios comerciales de su empresa o de todo el mundo. **Office Online:** (Word, Excel, PowerPoint, OneNote): Paquete office en línea, con ciertas limitantes de utilización.	A definir

3.1.10.3.1.9. Estabilización y cierre:

- Referentes a la migración de correo.
- Acompañamiento durante una semana posterior al cambio del registro de correo y entrada en operación de la plataforma de Office 365.
- Validación de las configuraciones de Exchange Online.

3.1.10.3.2. Implementación de la infraestructura Adicional:

Después, durante el desarrollo del contrato de Outsourcing se planeará la implementación de las aplicaciones opcionales en conjunto con el Instituto, tales como:

- SharePoint Online
- Microsoft Teams.
- Microsoft Forms
- Skype for Business
- Staff hub
- Microsoft Flow
- Yammer entre otros.

3.1.10.4. Mesa de ayuda

Este servicio deberá ser administrado bajo la guía del conjunto de buenas prácticas para el manejo de la infraestructura y operación de las tecnologías de información –ITIL® (Information Technology Infrastructure Library).

El contratista debe coordinar las actividades que permitan atender los requerimientos, problemas e inquietudes reportados por los usuarios del servicio, acerca de la operación de la infraestructura a cargo, incluido hardware y software, redes, insumos, papel y repuestos.

El proceso de administración de incidentes debe incluir la detección y el registro, clasificación y soporte inicial, investigación y diagnóstico, resolución y recuperación, cierre del incidente, monitoreo, trazabilidad y comunicación al usuario, contemplando escalamientos de soporte, todo controlado bajo una herramienta de software licenciado por el proveedor para uso exclusivo del Instituto Nacional de Cancerología, considerando escalamientos a segundo y tercer nivel de soporte.

El contratista debe certificar la legal adquisición del licenciamiento con derechos de uso para el INC.

3.1.10.4.1. Funciones Generales de la mesa de ayuda

Se refiere al personal y las herramientas que permiten garantizar la continuidad del servicio y la eficiente atención a los usuarios finales, frente a requerimientos relacionados con la infraestructura y servicios a cargo, lo cual incluye modalidad Outsourcing y modalidad administrados.

La administración del servicio debe incluir el control de inventarios de toda la infraestructura a cargo, hardware, software, redes, papel, repuestos y suministros, con registros detallados de ingresos y consumos. El control del inventario de software debe incluir el registro de licencias en uso frente al licenciamiento autorizado y documentación asociada. El contratista será responsable por la instalación de software no autorizado que se encuentre en la infraestructura a cargo, por lo cual deberá contar con las herramientas de monitoreo y control que le permitan realizar verificación constante. Mensualmente, con el informe de gestión se debe entregar el reporte del control de licenciamiento.

Todo el personal de la Mesa de Ayuda, y en particular el personal técnico (sin importar su modalidad), tienen a su cargo como mínimo las siguientes funciones transversales:

Soporte técnico a los usuarios finales y a las oficinas del INC en general, en el uso y funcionamiento de los equipos tecnológicos del INC y sus servicios y aplicaciones relacionadas, teniendo que instalarlos, actualizarlos, reinstalarlos y configurarlos según sea necesario.

Soporte técnico a los usuarios finales y a las oficinas del INC en general, en el uso y funcionamiento de herramientas comunes para ambiente PC: adecuada conexión y configuración de los computadores y su sistema operativo, ingreso a sesión de usuario, conexión a red, suite ofimática, internet, correo electrónico, antivirus y demás aplicaciones cliente, e instalarlas, actualizarlas, reinstalarlas y configurarlas según sea necesario.

Soporte técnico a los usuarios finales y a las oficinas del INC en general, en el uso y funcionamiento de los aplicativos del INC cliente o cliente servidor, misionales o administrativos, entre otros, e instalarlos, actualizarlos, reinstalarlos y configurarlos según sea necesario.

Actualización lógica del hardware (firmware) con las nuevas actualizaciones que se liberen o las que se requieran para el buen funcionamiento de los recursos tecnológicos.

Reubicación o reemplazo de equipos tecnológicos y relacionados.

Migración de datos de equipos antiguos a nuevos equipos asignados, bien sea por compra, arrendamiento o sustitución temporal.

Participación activa y soporte técnico a los usuarios finales y a las oficinas del INC en general, en tareas masivas y en aquellas que se derivan por cambios de la entidad, incluyendo traslados, migraciones y cambio de operadores tecnológicos. El Contratista deberá ofrecer una flexibilidad tal que esté en capacidad de proporcionar personal adicional para realizar dichas actividades, garantizando de esta forma la continuidad de los servicios informáticos.

El Contratista debe brindar soporte personalizado a los usuarios de correo, con los agentes necesarios para mantener los niveles de servicio. Incluye administración y soporte técnico y funcional especializado de las cuentas de correo y sus aplicaciones asociadas para los usuarios del INC, así como también la atención de requerimientos e incidentes de los aplicativos clientes de correo, correo en dispositivos móviles, y transversales de la plataforma, incluyendo el escalamiento de casos al fabricante.

Realización de las conexiones, configuraciones, instalaciones y pruebas de equipos tecnológicos cuando la Entidad lo requiera.

Acompañamiento técnico de apoyo a la entidad en las instalaciones de elementos nuevos o en arrendamiento que se definan en los diferentes proyectos de la organización, cuidando que dichas instalaciones se realicen en forma adecuada con respecto de los demás elementos o servicios tecnológicos del INC con los que guarden relación.

Mantenimiento preventivo de acuerdo a la programación establecida o por evidencia de su necesidad.

Todas las actividades de soporte, gestión tecnológica y garantías requeridas en las sedes y oficinas del INC.

El contratista tendrá a cargo la administración, gestión y control de los canales dedicados que actualmente tiene en uso, velando por su permanente funcionamiento. Entre sus actividades estará el reporte inmediato a los proveedores de este servicio en caso de fallo y el seguimiento permanente hasta su restablecimiento.

El personal profesional y técnico para la administración de la infraestructura instalada (modalidad de Outsourcing y modalidad administrados), estará en su totalidad a cargo del contratista. El personal técnico tendrá a su cargo la resolución de incidentes y el abastecimiento de insumos, papel y repuestos.

Se debe garantizar la entrega de reportes necesarios que permitan evaluar la calidad de los servicios TI, medir los consumos, verificar tendencias, entre otros.

El proponente deberá garantizar la evaluación permanente del grado de satisfacción de los usuarios a través de encuestas y reportar sus resultados al Instituto. Este proceso de evaluación deberá ser automatizado y diligenciado por el usuario desde su estación de trabajo, de manera que no medie interacción entre el técnico prestador del servicio y quien responde la encuesta. De igual manera, la calificación deberá ser reportada en el informe mensual.

Adicionalmente, de forma más específica el proponente debe:

- Estar altamente comprometido con la institución, garantizando excelente servicio al cliente y calidad en la prestación del servicio.
- Garantizar que instalará la totalidad de la infraestructura, puesta en operación (migrando la información de los equipos salientes a los equipos).
- Garantizar el suministro permanente de papel, insumos y repuestos, la instalación en cada equipo y la generación de los controles que este servicio demande.
- Garantizar la disponibilidad del software de apoyo. licenciado para uso del Instituto Nacional de Cancerología.
- Garantizar que cuenta con el software adecuado que permite controlar la gestión de la infraestructura instalada y los consumibles asociados, a la infraestructura de impresión.
- Garantizar que se cuenta con las herramientas apropiadas para controlar el servicio de impresión según cuotas de hoja impresas por usuario, perfiles, grupos y aplicativos, en la totalidad de impresoras instaladas.
- Garantizar el balanceo de cargas de impresión de acuerdo con los estudios de los procesos, volúmenes, evaluando el desempeño de los equipos frente a los volúmenes reales medidos.
- Garantizar que se tendrán equipos de contingencia en sitio, de las mismas características solicitadas, que garanticen la reposición inmediata de equipos que queden fuera de servicio.
- Controlar de forma permanente la información que asegure el mantenimiento a procesos y equipos.
- Apoyar la gestión de todos los aspectos relacionados con los sistemas de oficina, incluido soporte, capacitación sobre los aplicativos, computadores, divulgación y campañas de socialización que propendan por el uso adecuado de la tecnología.
- Garantizar la actualización permanente de la documentación técnica de todos los servicios TI a cargo.
- Garantizar la actualización permanente de los procesos actuales y apoyar nuevas formas de trabajo, cumpliendo con los lineamientos de la oficina de Calidad del INC.
- Garantizar el aprovisionamiento, seguimiento, sustitución de hardware y software de la infraestructura a cargo, asegurando suministro, calidad y cumplimiento.

- Responder con rapidez a cambios de infraestructura física y/o lógica, mediante procesos de distribución masiva de los equipos de cómputo de usuario final, cumpliendo los estándares y políticas informáticas.
- Contar con soporte especializado, en sitio o fuera de las instalaciones para asistir al personal asignado al INC.
- Garantizar el control de licenciamiento autorizado frente al licenciamiento en uso, tanto de las licencias de propiedad del INC como las suministradas por el contratista.
- Garantizar la generación de informes periódicos de gestión e indicadores de consumo por usuario y centro de costo en temas de impresión.
- Garantizar la generación de estadística de desempeño y disponibilidad del servicio.
- Garantizar el desarrollo y la mejora de los servicios en la plataforma de red y servidores para optimizar los recursos, en procura de una administración eficiente de los sistemas de autenticación.
- Gestionar las garantías de los equipos de red, directamente con los fabricantes de los mismos, garantizando un servicio de red sin interrupciones.
- Documentar la totalidad de los puntos de red y fibras tendidas, instaladas en desarrollo del contrato junto con el inventario de los mismos (planos y ducterías).
- Instalar o trasladar puntos de red sencillos, categoría 6A debidamente certificados, en los sitios donde sean requeridos que no impliquen cambios sobre la infraestructura física u obra civil. La instalación de estos puntos incluirá el material requerido el cual será suministrado por parte del contratista. Se estiman inicialmente una cantidad de 100 puntos nuevos instalados, y 100 reubicaciones. Estos puntos se liquidaran según demanda.
- Realizar el 100% de las actividades técnicas necesarias para garantizar el correcto funcionamiento de la red de voz y datos a nivel físico y lógico, lo anterior incluye mantenimiento preventivo y correctivo a los centros de cableado, equipos activos, enlaces de fibra, cobre y la certificación de puntos y enlaces en caso de ser necesario.
- Garantizar mecanismos de seguridad que protejan los equipos de cómputo e impresión.
- Desde el inicio de instalación, el contratista debe garantizar la conformación de una base de datos que permita el registro, organización, gestión y actualización de los datos de configuración de cada componente que hace parte de la infraestructura a cargo y ésta deberá ser actualizada cada vez que sea necesario, contando previamente con los avales de los supervisores técnicos del contrato.
- Garantizar que las modificaciones sobre servicios o cambios de políticas serán concertados con los supervisores técnicos del contrato.
- El proponente debe garantizar el licenciamiento legalmente adquirido con derecho de uso para el Instituto Nacional de Cancerología, tanto para equipos en la modalidad de Outsourcing como en la modalidad administrados:

    - Software para administración de Mesa de Ayuda, que garantice escalamiento y trazabilidad de los incidentes reportados y registro directamente por parte de los usuarios finales.
    - Software de gestión de inventario que garantice mantener la información completa y actualizada de los inventarios de software y hardware a cargo y en tiempo real.
    - Contar con el software que permita brindar soporte remoto a usuarios.
    - Software para controlar impresiones de forma automática, donde se especifique cantidad de impresiones por usuario, área y detalle de documentos, con capacidad de evaluar cantidades de papel entregado frente a cantidades de papel utilizado.
    - Sistemas operativos con un sistema de actualización, integración y soporte bajo plataforma WSUS (Windows Server Update Services).
    - Software de oficina el cual deberá instalarse en equipos desktop, portátiles, en la modalidad de Outsourcing y en la modalidad administrada. A partir de este nuevo contrato el Instituto adoptará el modelo de software como servicio de la plataforma Office 365. Para lo cual el contratista deberá suministrar el licenciamiento adecuado para el INC, y que cumpla con los requerimientos específicos consignados en la hoja Licenciamiento del archivo Anexo No. 7 TecnicosInvitacionPublica_Outsourcing.xlsx.
    - Actualmente el INC cuenta con 360 licencias de Microsoft office Estándar y 59 licencias de Microsoft office profesional las cuales deberán ser utilizadas y además complementar en número de licencias adicionales para cubrir 100% de la infraestructura de equipos con usuario genérico de acuerdo a la hoja Licenciamiento del archivo Anexo No. 7 TecnicosInvitacionPublica_Outsourcing.xlsx.
    - Software Antivirus, con consola centralizada. Considerar equipos desktop, portátiles, servidores, máquinas virtuales, en la modalidad de Outsourcing y en la modalidad administrada.

- Herramienta DLP (Data Lost Prevention) para End Points, y servicio DLP para correo electrónico, cuya instalación se definirá según cronograma acordado entre las partes.
- El producto antivirus que seleccione el proveedor, deberá estar dentro del cuadrante de Gartner para “Endpoint Protection platforms” para el año 2018,
- Software para compresión/descompresión archivos con soporte para compresión RAR.
- Tener en cuenta la hoja Licenciamiento del archivo Anexo No. 7 TecnicosInvitacionPublica_Outsourcing.xlsx.

Se debe garantizar la presencia de un coordinador del servicio en sitio, tiempo completo, que cuente con el perfil profesional y acredite conocimiento y experiencia previa para coordinar toda la gestión y apoyar los procesos internos que se deriven de los servicios a contratar. Esta persona debe contar mínimo con certificación ITIL Intermediate®.

3.1.10.4.2. Alcance Mesa de ayuda

El servicio de mesa de ayuda está orientado a que sea el punto de contacto inicial del usuario final a través del cual se reportan los incidentes. El Instituto usará este servicio para canalizar solicitudes de TI, pero además será utilizado para gestionar temas adicionales que requiera el INC con el objetivo de tener trazabilidad de las solicitudes.

Teniendo en cuenta que el Instituto Nacional de Cancerología – Empresa Social de Estado, presta sus servicios 24/7, y se presentan eventos que pueden afectar el normal funcionamiento de los servicios, por lo tanto, se considera necesario contar con la mesa de ayuda que adicionalmente a los servicios de sistemas, apoye de las áreas que se describen más adelante, así:

- Recibir llamadas
- Clasificar el servicio
- Registrar los datos de la solicitud con número de ficha o ticket.
- Enviar la solicitud al área correspondiente.
- Recibe el reporte de resolución.
- Envía reporte al solicitante del estado del trámite.
- Emitir reportes permanentes del estado de avance de las solicitudes realizadas y disponer de un archivo de consulta para los usuarios.

Las llamadas que se reciban deben estar relacionadas con los siguientes servicios y deben ser atendidas todos los días 24 x 7 (de lunes a domingo, incluyendo festivos).

1. Servicios de TI: Se deben registrar eventos que se presenten en los horarios mencionados y que afecten el normal funcionamiento de los servicios de TI, en la actualidad se atienden en promedio mes, 1700 órdenes. De las cuales 1200 son directamente atendidas por el personal de mesa de ayuda, y 500 son referentes al sistema de información SAP, las cuales son atendidas por personal interno del INC. Estos eventos se atienden con base en los tiempos definidos en los Acuerdos de niveles de servicio.

2. Área de Infraestructura: Se deben registrar eventos que se presenten en los horarios mencionados y que afecten el normal funcionamiento de los servicios, en la actualidad se atienden en promedio mes, 560 órdenes. (Estos eventos deben ser notificados al día siguiente al Coordinador de Grupo de Infraestructura)

3. Área de Tecnología Biomédica. Llamadas que se puedan presentar con ocasión a fallas en equipos biomédicos, en la actualidad se atienden en promedio mes 150 solicitudes de servicios. (Estos eventos deben ser reportados al día siguiente a la Coordinadora de Grupo Área de Tecnología Biomédica y Almacén).

4. Seguridad y Salud en el trabajo: Eventos de accidentes de trabajo, en la actualidad se atienden en promedio mes 4 accidentes de trabajo (Estos eventos deben ser reportados al día siguiente a la Coordinadora de Grupo de Seguridad y salud en el trabajo)

5. Subdirección Administrativa y financiera: En caso de requerirse el apoyo del área administrativa del Instituto por los servicios en estos horarios, se dejarán registrados

los números telefónicos del contacto de turno, quien atenderá la llamada para brindar el apoyo solicitado.

6. Subdirección de Atención Médica y Docencia: En caso de ser reportados caso de ausencia de personal médico o enfermería, se dejarán registrados los números telefónicos del contacto de turno; quien atenderá la llamada para brindar el apoyo solicitado.

3.1.10.4.3. Puntos de Contacto

El centro de llamadas de la Mesa de Ayuda brindará soporte de primer nivel a los funcionarios del INC mediante los siguientes canales de atención:

- Línea 7000, línea directa desde cualquier extensión telefónica del INC.
- Mediante envío de correo electrónico reportando incidentes a la dirección sima@cancer.gov.co
- Mediante herramienta de gestión de mesa de ayuda, con interfaz para usuario final.
- Mediante los canales de atención adicional que el Instituto defina durante la duración del contrato.

El soporte del centro de llamadas será brindado a través de los medios anteriormente descritos, por el equipo de soporte, cuyos roles y perfiles se describen en el apartado 3.1.10.5.

Sin perjuicio de lo anterior, el Contratista deberá adicionar todo el personal que requiera para dar soporte al usuario por los medios mencionados cumpliendo con los niveles de servicio.

La mesa de ayuda prestará sus servicios con disponibilidad plena de lunes a viernes de 7 a.m. a 5 p.m. Adicionalmente, prestará sus servicios en el horario de 5pm a 7 am, con la cantidad de agentes necesaria para mantener los niveles de servicio. Lo anterior teniendo en cuenta que los fines de semana la mayoría de las áreas administrativas no labora, sin embargo, las áreas asistenciales se encuentran en permanente ejercicio las 24 horas del día. Para lo anterior, el Contratista podrá hacer los turnos con los que cumpla en todo momento con los niveles de servicio requeridos por la entidad.

3.1.10.4.4. Soporte en sitio

El contratista debe garantizar que se tendrá el grupo de soporte técnico de acuerdo con los perfiles requeridos para que preste su servicio directamente en las instalaciones del Instituto Nacional de Cancerología descritas en el ítem 1.3. Con el fin de atender todas las incidencias, realizar las instalaciones de software, configuraciones de hardware, cambio de partes, gestión y control de garantías, suministro de insumos, papel y repuestos, entre otras actividades que se requieran, para garantizar la solución de problemas de infraestructura TI en el menor tiempo posible con la mayor calidad esperada.

El grupo de soporte en sitio debe estar en las instalaciones del Instituto para brindar el soporte de primer y segundo nivel, en el horario de lunes a domingo, durante las veinticuatro (24) horas, para atender los servicios en horario diurno y nocturno.

3.1.10.4.5. Gestión de Garantías

El Proveedor debe garantizar que los equipos tecnológicos entregados al INC, tienen fecha de inicio de garantía de fábrica a partir de la fecha entrega de los equipos. Al momento de la entrega de los equipos, el Proveedor debe entregar el listado de serial de los equipos y los medios a través de los cuales El INC podrá verificar la fecha de inicio de la garantía de los mismos. Esta información podrá ser verificada por El INC a través de la herramienta de gestión de inventarios, mesa de ayuda, del portal Web o persona de contacto del fabricante.

3.1.10.4.6. Suministros y Repuestos

Se debe garantizar el suministro permanente de todos los consumibles y repuestos requeridos para la operación del servicio, incluida la papelería y tóner para las impresoras en las modalidades de Outsourcing y administradas.

Adicionalmente, se debe garantizar el suministro de todas las herramientas y materiales necesarios para el desarrollo de las actividades de redes, mantenimiento preventivo, mantenimiento correctivo, y actividades de mesa de ayuda (equipos de cómputo, herramientas de diagnóstico físico y lógico, teléfonos, entre otros) para el grupo de soporte en INC.

La propuesta deberá informar en detalle los mecanismos con los cuales se administrará la logística para el aprovisionamiento de suministros que requiera la infraestructura que se instale en el Instituto, de manera que se garantice abastecimiento permanente e ininterrumpido. Se debe garantizar la permanencia de un stock de insumos en sitio que garanticen óptimos niveles de servicio.

Los suministros deben ser nuevos y de buena calidad. En los casos que se evidencien suministros de consumibles de dudosa calidad se procederá a realizar el descuento respectivo del equipo que presta el servicio al momento de liquidar el pago mensual.

Al reemplazar el tóner de una impresora en uso, el insumo en su empaque de fábrica, sin destapar, debe trasladarse al área en la que se encuentre ubicada la impresora, con el fin de hacer evidente ante el usuario, que se está haciendo el reemplazo por un insumo nuevo. Al concluir el cambio, el usuario certificará en el formato correspondiente el reemplazo realizado. El técnico procederá a retirar el tóner agotado y realizar el procedimiento de descarte respectivo.

3.1.10.4.7. Traslado De Equipos Tecnológicos Durante La Ejecución del contrato.
El INC durante la ejecución del Contrato, podrá en caso que así lo requiera, trasladar los equipos tecnológicos a las áreas o sedes que se requiera sin cargo adicional.

3.1.10.4.8. Informes de gestión
El proponente debe garantizar por defecto la entrega de informes estadísticos mensuales en forma gráfica y en reporte digital. Adicionalmente, el suministro de informes por demanda sobre información de las áreas involucradas.

El contratista deberá entregar documentación formal de la solución de los incidentes y problemas e informes mensuales de la operación. Entregar un informe mensual de gestión de la operación.

Para el proceso de liquidación mensual será requisito la presentación del informe de gestión, la relación de firmas de los usuarios a quienes se les hizo entrega de papel y cambio de insumos en sus impresoras, reemplazo de equipos por contingencia, reemplazo de partes y actas de instalación inicial. De igual forma, se debe suministrar el informe mensual de control de licencias, reporte actualizado de inventario, estado actual de la infraestructura de redes, servidores y cambios en personal de apoyo.

Entregar un informe mensual de gestión de seguridad informática. Entregar un informe mensual de capacidad y disponibilidad de servidores y plataformas tecnológicas.

Entregar documentación formal de la solución de los incidentes y problemas e informes mensuales de la operación. Entregar un informe mensual de gestión de cambio dentro de las plataformas administradas. Adicionalmente, se debe presentar la evaluación de las encuestas realizadas y el análisis de impacto de las campañas que se adelanten a cargo del servicio de Outsourcing.

3.1.10.4.9. Acuerdos de Niveles de Servicio
Los Acuerdos de Niveles de Servicio (ANS) se formalizarán a partir de la información consignada en el documento Anexo_NivelesdeServicio.xlsx.

La entidad actualizará periódicamente los requerimientos del servicio con el fin de mantener su vigencia y alineamiento con las necesidades de los mismos. Estas actualizaciones pueden generar requerimientos menores o adicionales de servicio de carácter temporal o definitivo.

Todos los casos de solicitudes o causales de incumplimiento, son acumulables al corte del mes siguiente, hasta tanto no se haya restaurado el servicio o resuelto el caso.

Terminada la etapa de transición, empezaran a correr los ANS en la etapa de operación.

Los indicadores NSO (Nivel de Servicio Objetivo) y NSM (Nivel de Servicio Mínimo) iniciales, que se deben cumplir por parte del Contratista en la prestación de los servicios, y se consignan en el documento Anexo_NivelesdeServicio.xlsx.

Estos indicadores podrán ser actualizados periódicamente y de común acuerdo entre la Entidad y el Contratista, de conformidad con un análisis previo en materia de arquitectura tecnológica y oportunidades de mejoramiento disponibles.

3.1.10.4.9.1. Procedimiento para determinación del nivel de cumplimiento de ANS
El Nivel de Cumplimiento de los ANS, se aplicará bajo el siguiente procedimiento

Mensualmente el Contratista presentará los informes de desempeño para el servicio de Mesa de Ayuda, generados a partir de la herramienta de gestión, dentro de los cinco (5) primeros días calendarios del mes siguiente al mes que se vaya a facturar.

La Entidad y el Contratista analizarán conjuntamente el cumplimiento de lo acordado.

En el documento Anexo_NivelesdeServicio.xlsx se relacionan el Nivel de Servicio Objetivo (NSO) y Nivel de Servicio Mínimo (NSM) aplicables a la prestación del servicio de Mesa de Ayuda, en cuanto se refiere al cumplimiento de los ANS.

3.1.10.4.9.2. Valoración del nivel de satisfacción de los usuarios

Para el servicio de Mesa de Ayuda, la evaluación del nivel de satisfacción de los usuarios, se realizará utilizando fuentes formales de información, métodos cuantitativos (**encuestas, entrevistas**) y procedimientos estadísticos que garanticen la confiabilidad y precisión de ésta.

Esta valoración será realizada de manera mensual durante la ejecución del contrato. Los costos de los estudios serán asumidos por el Contratista. Las encuestas se harán como mínimo a una muestra del **20%** de la población, total de usuarios que reciben el servicio.

Nota: El Contratista garantizará el cumplimiento de los ANS definidos para cada servicio, para lo cual implementará el modelo de servicio y los mecanismos que apoyen la prestación de los mismos.

3.1.10.5. Perfiles del Personal de Soporte y Mesa de ayuda

Como mínimo, el grupo de trabajo en sitio debe estar conformado por los siguientes roles y cada uno de ellos debe ser desempeñado por personas diferentes, es decir, una misma persona no podrá asumir más de un rol. Con el animo de facilitar la participación, el oferente que resulte seleccionado debera presentar las hojas de vida de los perfiles solicitados al inicio del contrato. Los perfiles deben cumplir con todas las especificaciones. En caso de no cumplirse se aplicaran las clausulas de incumplimiento.

3.1.10.5.1. Coordinador de servicios IT

- Un (1) profesional graduado en ingeniería de sistemas y/o ingeniería electrónica / telecomunicaciones, Ingeniería Industrial o Administración de empresas y/o carreras afines., Especialista en gerencia de proyectos o su equivalente certificado PMP. Debe contar con certificación de ITIL® Intermediate. Debe contar con conocimientos de administración de Windows Server y office 365 (nivel profesional), Linux (nivel profesional), Redes (nivel profesional). Experiencia en manejo herramienta de Help Desk y gestión de incidentes basada en ITIL. Este profesional debe contar con experiencia en gerencia de mesas de servicio TI, por cinco (5) o más años, en empresas con más de 600 usuarios o como coordinador del servicio de Outsourcing o mesa de ayuda. Este profesional será el encargado de coordinar las actividades del servicio de Outsourcing en el INC y será el interlocutor válido en sitio representando el contratista ante los supervisores designados por el Instituto.

3.1.10.5.2. Administrador de Redes de voz y Datos

- Un (1) profesional graduado en ingeniería de sistemas y/o ingeniería electrónica y/o ingeniería en telecomunicaciones, y/o carreras afines. con certificación en fundamentos ITIL®. Deberá contar con certificación CCNA y/o profesional Técnico Acreditado de HPE (ATP). **se acepta certificaciones equivalentes al CCNA** .Debe contar con certificación IPV6 Forum. Minimo Certified System Administrator Gold o IPV6 Forum Certified Network Engineer administrator Gold. Este profesional debe contar con experiencia certificada como administrador de redes de voz y datos, por tres (3) o más años, en empresas con más de 600 usuarios. certificaciones que no cumplan con estos requisitos no serán tomadas en cuenta. Este profesional asumirá el rol de administrador principal de redes de datos en INC.

3.1.10.5.3. Administrador Plataforma Servidores y Ofimática.

- Un (1) profesional graduado en ingeniería de sistemas y/o ingeniería electrónica, o telecomunicaciones, y/o carreras afines. certificado en MCSE Experto en soluciones de productividad (MCSA Office 365, MCSA Windows Server 2012, MCSA Windows Server 2016), y con experiencia en administración de plataformas Linux. Debe contar con certificación en fundamentos ITIL® vigente. Este profesional debe contar con experiencia certificada como administrador de plataformas Windows-server y Office 365, por tres (3) o más años, en empresas con más de 600 usuarios. Certificaciones que no cumplan con estos requisitos no serán tomadas en cuenta. Este profesional asumirá el rol de administrador de plataformas Windows y correo electrónico bajo la plataforma Office 365, además de las plataformas Linux existentes, (implica tener experticia en, virtualización, storage, networking, administración sobre sistemas WinServer, Active Directory, DHCP, DNS, WSUS y tener experiencia comprobada en integración de tecnologías y administración de sistemas que corran sobre plataformas Linux). Si el proveedor considera que para cumplir este rol requiere más de un administrador lo puede ofertar.

3.1.10.5.4. Administrador de Seguridad Informática

- Un (1) profesional graduado en ingeniería de sistemas y/o ingeniería electrónica, o ingeniería de telecomunicaciones y/o carreras afines, con conocimiento certificado en marcos de trabajo de seguridad de la información y/o especializaciones afines a la seguridad de la información registradas en el Sistema Nacional de Información de la Educación Superior (SNIES). Certificación de implementación y administración del fabricante de Firewall de siguiente generación o appliance de seguridad ofertado. Certificación en implementación y administración de fabricante de appliance de análisis de eventos y correlación de riesgo ofertado. Experiencia mínima de 3 años en administración de la plataforma de seguridad informática ofertada. Experiencia mínima de 2 años en administración de consola centralizada de antivirus ofertada. Con certificación en fundamentos ITIL® v3 o superior reconocido por organismo certificador autorizado. Conocimientos certificados de seguridad sobre IPV6. Este profesional asumirá el rol de administrador de las plataformas de seguridad informática (Firewall de nueva generación, ,seguridad perimetral, restricciones de navegación, IPS, WAF, DDOS, appliance analizador de eventos, VPNs punto a punto y VPNs de usuario), plataforma de seguridad de correo electrónico (antispam basado en firmas, Data Loss Prevention (DLP) para OFFICE 365) seguridad Endpoint (Consola centralizada de Antivirus, DLP para Endpoints), Network Access Control - NAC, políticas de active Directory), seguridad criptográfica (entidad certificadora CAServer), y monitoreo de seguridad (Monitores de disponibilidad, gestión de alerta de seguridad, monitoreo y solución de vulnerabilidades de seguridad informática) d). Este profesional debe contar con experiencia certificada como administrador de plataformas de seguridad informática, por cinco (5) o más años, en empresas con más de 600 usuarios. Certificaciones que no cumplan con estos requisitos no serán tomadas en cuenta. Si el proveedor considera que para cumplir este rol requiere más de un administrador lo puede ofertar.

3.1.10.5.5. Tecnólogo de Redes de Voz y Datos

- Un (1) tecnólogo en redes, electrónica o telecomunicaciones y/o carreras afines., con curso certificado CCNA y/o HPE Networking. Se acepta certificaciones equivalentes al CCNA Con certificación en fundamentos ITIL® v3 o superior reconocido por organismo certificador autorizado. Esta persona debe contar con experiencia certificada como tecnólogo de redes de datos, por tres (3) o más años. Certificaciones que no cumplan con estos requisitos no serán tomadas en cuenta. Este tecnólogo debe contar con experiencia certificada como administrador de redes de datos, por uno (1) o más años, en empresas con más de 50 usuarios. Este profesional asumirá el rol de tecnólogo en redes de datos del INC, y prestara apoyo a todas las funciones que desempeñe al administrador de la red.

3.1.10.5.6. Técnico Y/O Tecnólogo Soporte TI Nivel 2 – Office 365

- Un (1) técnico de soporte Nivel 2, con título de Técnico o de Tecnólogo en áreas de Informática y/o Electrónica, y/o Telecomunicaciones y/o Soporte y Mantenimiento y/o carreras afines. (se aceptan estudiantes de Ingeniería de Sistemas, y/o Electrónica, Telemática y/o Telecomunicaciones, que estén cursando mínimo 6to semestre), y con certificación en Fundamentos de ITIL V.3, que tenga experiencia de mínimo 2 años en la administración gestión y soporte de plataforma Office 365. Esta persona debe contar con experiencia certificada como técnicos de soporte de Office 365. Este personal se encargara de brindar soporte a la plataforma office 365 que incluye cuentas de correo electrónico MS Office 365 (Outlook) y sus herramientas asociadas en la nube (OneDrive, Skype for Business, Yammer, Teams, SharePoint, etc.), para los usuarios del INC, así como también la atención de requerimientos e incidentes de los aplicativos clientes de correo, correo en dispositivos móviles, y transversales de la plataforma, incluyendo el escalamiento de casos al fabricante. Certificaciones que no cumplan con estos requisitos no serán tomadas en cuenta.

- Seis (6) de soporte técnico de Nivel 2, con título de Técnico o de Tecnólogo en áreas de Informática y/o Electrónica, y/o Telecomunicaciones y/o Soporte y Mantenimiento, con conocimiento básico en equipos Apple. (se aceptan estudiantes de Ingeniería de Sistemas, y/o Electrónica, Telemática y/o Telecomunicaciones, que estén cursando mínimo 6to semestre), y con certificación en Fundamentos de ITIL V.3. Deberán contar con experiencia certificada de (2) años o más como técnico y/o tecnólogo en soporte TI. Certificaciones que no cumplan con estos requisitos no serán tomadas en cuenta. Estas personas asumirán el rol de técnico de soporte TI en INC.

3.1.10.5.7. Técnicos Y/O Tecnólogos Soporte TI Nivel 1

- Dos (2) agentes de nivel 1, con título de Técnico o de Tecnólogo en áreas de Informática y/o, Electrónica y/o Telecomunicaciones y/o Soporte y Mantenimiento y/o carreras afines. Se aceptan estudiantes de Ingeniería de Sistemas y/o Electrónica y/o Telemática y/o

Telecomunicaciones, que estén cursando mínimo 6to semestre. Debe tener Certificación en Fundamentos de ITIL V.3. y con experiencia mínima de 2 años en atención telefónica y soporte técnico remoto de equipos informáticos y/o cargos similares. Certificaciones que no cumplan con estos requisitos no serán tomadas en cuenta. Estas personas asumirán el rol de operadores telefónicos de mesa de ayuda en INC.

Ante la ausencia de algunos de los perfiles solicitados en sitio deba ausentarse por permiso, incapacidad, vacaciones o descanso programado, el proveedor deberá garantizar el personal que supla la ausencia con los perfiles adecuados, y este deberá ser reemplazo por una persona que cuente con el entrenamiento adecuado, del mismo perfil o superior de la persona. Al momento de presentar este tipo de eventualidades, se deberá informar a la supervisión técnica del contrato el evento y presentar la hoja de vida de quien realizará el reemplazo. En caso de que la ausencia se prolongué por más de 3 días, el proveedor deberá garantizar la operación y los servicios contratados, no obstante, lo anterior el INC realizará el descuento correspondiente proporcional a los costos de la oferta de acuerdo a la información de la hoja CostoProductosServicio del archivo Anexo No. 8 CostosInvitacionPublica_Outsourcing.xlsx),

El personal que hará parte del equipo de trabajo en INC debe cumplir con las siguientes normas:

- Uso de prendas de vestir de la compañía que representa, con el logotipo y nombre de la misma (se sugiere chaleco, chaqueta o camisa).
- Portar carnet de la compañía que representa.
- El personal de servicio de Outsourcing debe contar con el apoyo de un sistema de comunicaciones que permita la fácil ubicación y comunicación entre el grupo y el Instituto.

El contratista debe garantizar que su personal contará con la dotación de elementos de protección personal que las normas de seguridad industrial obligan para el desempeño de sus labores.

3.1.10.6. Servicios de Backup

3.1.10.6.1. Alcance

El contratista deberá suministrar un servicio de gestión de backup en sitio para la gestión de copias de seguridad y restauración de servidores descritos en los EMR-219 para toda la información y los servicios físicos o virtuales que estos soportan, y para la configuración de todos los servicios y sistemas ofertados y administrados por el contratista para mitigar los efectos de un posible incidente de indisponibilidad, u ocurrencia de un desastre natural.

3.1.10.6.2. Responsabilidad

El contratista deberá suministrar y administrar el servicio integral de respaldo (hardware, software, licencias, estrategia de backup, administración, medios de respaldo, resguardo externo seguro), que garantice el respaldo y restauración de todas las plataformas tecnológicas suministradas y administradas por el contratista, que se encuentren en producción durante el contrato. El resguardo externo seguro hace referencia a que el contratista debe proveer los medios, realizar periódicamente, trasportar, mantener y custodiar copias de seguridad para almacenamiento externo bajo su custodia o empresa especializado para garantizar que el backup esté disponible en caso de ocurrencia de un desastre mayor dentro del datacenter del INC.

El contratista deberá proveer una estrategia de recuperación rápida que permita proveer/devolver el servicio a los usuarios casi inmediatamente y en forma sencilla. Dentro de esta estrategia el contratista debe suministrar los medios de respaldo necesarios para cubrir todo el volumen de datos a respaldar.

El contratista durante la etapa de migración deberá administrar el control de copias de respaldo de la información contenida en los equipos de usuario final, para lo cual se deberá implementar un repositorio de red para el almacenamiento correspondiente, definir y socializar el procedimiento correspondiente y tener el control detallado de la gestión de copias. La infraestructura para realizar la actividad deberá ser suministrada por el proveedor de forma temporal mientras dure la migración.

3.1.10.6.3. Características mínimas de sistema de Backup

El sistema de Backup debe cumplir con las siguientes características mínimas:

- La solución deberá incluir funcionalidades de respaldo (backup) y replicación integradas en una única solución; incluyendo vuelta atrás (rollback) de réplicas y replicación desde y hacia la infraestructura virtualizada.

- La solución no deberá necesitar de la instalación de agentes para poder realizar sus tareas de respaldo, recuperación y replicación de máquinas virtuales.
- Deberá poder realizar respaldos sin detener las máquinas virtuales, y sin generar una merma en su performance, facilitando las tareas de respaldo (backup) y migraciones en conjunto.
- Deberá ser capaz de comprender las máquinas virtuales como objetos del entorno virtual y respaldar las configuraciones de las mismas, al margen de los datos propios de las máquinas.
- Deberá ser capaz de respaldar de forma indistinta una máquina virtual completa o discos virtuales específicos de una máquina virtual.
- Deberá proveer una herramienta de gestión de archivos para los administradores de máquinas virtuales en la consola del operador.
- La solución deberá ofrecer múltiples estrategias y opciones de transporte de datos para las tareas de respaldo.
- Deberá proporcionar un control centralizado del despliegue distribuido, para esto deberá incluir una consola web que provea una vista consolidada de su despliegue distribuido y federación de múltiples servidores de respaldo (backup), informes centralizados, alertas consolidadas y restauración de auto servicio de máquinas virtuales y a nivel de sistema de archivos (granular), con asignación de permisos sobre máquinas virtuales individuales.
- Deberá contar con la tecnología de deduplicación (técnica de compresión para eliminar copias duplicadas de datos repetidos) para lograr un ahorro de espacio de almacenamiento para los respaldo (backup).
- La solución no deberá requerir hardware específico para alcanzar la de-duplicación y compresión de la información fuera de los requerimientos estándar de cualquier software, y específicos para el caso.
- Deberá ser capaz de realizar replicas en otros sitios o infraestructuras desde los respaldos realizados.
- El sistema recuperación de backup debe permitir el inicio de la máquina virtual que haya fallado, directamente desde el archivo de respaldo (backup) en el almacenamiento habitual del respaldo (backup).
- La recuperación instantánea de las máquinas virtuales, deberá permitir más de una máquina virtual y/o punto de restauración en simultáneo para la disponibilización del punto de recuperación funcional, permitiendo así, tener múltiples puntos en el tiempo de una o más máquinas virtuales funcionando.
- Luego de la recuperación rápida, se deberá poder realizar una restauración total sin interrupciones del servicio. Se pretende que el trabajo realizado por los usuarios no deberá verse afectada al migrar sus máquinas virtuales desde el respaldo (backup) hasta el almacenamiento de producción. Deberá poseer una opción de recuperación instantánea de archivos que se encuentren dentro de los respaldos (backup) y replicaciones de las máquinas virtuales. Lo que debe permitir acceder a los contenidos de los discos virtuales de dichas máquinas sin necesidad de recuperar el respaldo (backup) completo y reiniciar desde el mismo la máquina virtual.
- Deberá incluir un asistente para la recuperación instantánea a nivel de archivos en los sistemas de archivos más utilizados de mínimo Windows, Linux, Solaris, BSD o MacOS
- Deberá poder crear un índice (catálogo) de todos los archivos que sean manejados por el sistema operativo Windows, cuando este sea el sistema operativo que ejecute dentro de una máquina virtual del que se ha realizado un respaldo (backup).
- Deberá poder realizar búsquedas rápidas mediante índices de los archivos que sean manejados por un sistema operativo Windows, cuando este sea el sistema operativo que ejecute dentro de una máquina virtual del que se ha realizado un respaldo (backup).
- Deberá asegurar la consistencia de aplicaciones transaccionales en forma automática por medio de la Integración con Microsoft VSS, dentro de sistemas operativos Windows.
- Deberá poder realizar el truncado de las bitácoras transaccionales (Transaction logs) para máquinas virtuales con SQL Server.
- Deberá poder realizar notificaciones por correo, SNMP o a través de los atributos de la máquina virtual del resultado de la ejecución de sus trabajos.

- Se deberá poder recuperar a nivel de objetos de cualquier aplicación virtualizada, en cualquier sistema operativo, utilizando las herramientas de gestión de aplicaciones existentes.
- Deberá incluir herramientas de fácil recuperación guiada mediante el cual los administradores de servidores de servicio de directorio, tales como, Microsoft Active Directory, pueden utilizar para recuperar objetos individuales, tales como usuarios, grupos, etc. Sin necesidad de recuperar los archivos de la máquina virtual como un todo y reiniciar la misma.
- Deberá incluir herramientas de fácil recuperación guiada mediante el cual los administradores de servidores de bases de datos Microsoft SQL Server, puedan recuperar objetos individuales, tales como tablas y registros. Sin necesidad de recuperar los archivos de la máquina virtual como un todo y reiniciar la misma
- Deberá poder ofrecer confiabilidad en un 100% en el inicio correcto de todas sus máquinas virtuales respaldadas y en el funcionamiento del rol que cumple dichas máquinas virtuales (DNS Server, Domain Controller, Mail Server, SQL Server, etc) al momento de la recuperación.
- Deberá poder crear una copia de trabajo del entorno de producción de cualquier estado anterior para la resolución de problemas, pruebas de procedimientos, capacitación, etc. ejecutando una o varias máquinas virtuales desde el archivo de respaldo (backup) en un entorno aislado, sin necesidad de más espacio de almacenamiento y sin modificar el respaldo (backup).
- Deberá ofrecer el archivado en cinta, soportando VTL (Virtual Tape Libraries), biblioteca de cintas y drives independientes.
- Deberá ofrecer Trabajos de Copia de Backup con implementación de políticas de retención.
- Deberá soportar las últimas versiones disponibles de los hipervisores más populares de mercado a la fecha: VMWare vSphere 5.5 y Microsoft Hyper-V 2012 R2.
- No deberá requerir licencias independientes para las actividades de respaldo, recuperación y replicación.
- No deberá requerir licencias independientes para el respaldo y recuperación granular guiada y consistente de software (sin montar ambientes temporales) para:
    - Microsoft Active Directory
    - Microsoft SQL Server 2008 en adelante
- Deberá ofrecer la posibilidad de almacenar los respaldos de forma encriptada, así como asegurar el tránsito de la información bajo este esquema.
- Deberá permitir la delegación de tareas de recuperación, a nivel de elementos de aplicación, hacia otros usuarios, de forma tal a poder descargar la cantidad de maniobras a ejecutar por el administrador de la plataforma.
- Deberá disponer de funcionalidades integradas que permitan la selección de un destino de almacenamiento de respaldos que pueda estar alojado en un proveedor de servicios en la nube.
- Deberá integrar una solución unificada de monitoreo de ambientes virtuales y respaldos de forma de poder co-relacionar ambas infraestructuras, las alarmas y reportes.
- Deberá ofrecer un conjunto de reportes capaces de presentar información de tipo:
    - Reportes que permitan la planificación de la capacidad.
    - Reportes que permitan la determinación de inefectividad en el uso de recursos.
    - Reportes que faciliten la visibilidad de tendencias negativas y anomalías.
    - Tableros de controles claros, presentables e integrables en sitios web.
- Deberá poseer la capacidad de generar segregación de acceso según el perfil del usuario, al monitoreo de la infraestructura conectada a la plataforma.
- Deberá co-relacionar la ejecución de trabajos de respaldo y replica con los objetos del entorno virtual.
- Deberá ofrecer la capacidad de reportar el cumplimiento de políticas de protección de datos y disponibilidad acorde a parámetros definidos.
- Deberá poseer base de conocimiento integrada en las alarmas, aunque también debe soportar la personalización de las alarmas y descripciones de base de conocimiento.

3.1.10.6.4. **Administración y operación de sistema de Backup**

El contratista administrará la solución de backup ofertada para mantener respaldada adecuadamente toda la infraestructura tecnológica y de seguridad informática instalada.

El contratista debe ejecutar las siguientes actividades:

- Instalar, configurar y Optimizar la plataforma de respaldo ofertada y los procesos asociados.
- Diseñar y documentar las rutinas y frecuencias de los respaldos.
- Administrar la programación y ejecución de los respaldos.
- Realizar la ejecución de cambios de rutinas y frecuencias de los respaldos.
- Atender y ejecutar los requerimientos de respaldos y restauraciones demandadas a solicitud del INC. Ejecutar las restauraciones dentro de los plazos que se estipulen.
- Validar la ejecución completa y la integridad de los respaldos programados automáticamente en el sistema de backup, solucionando los errores en la ejecución de los respaldos.
- Garantizar el funcionamiento y disponibilidad 7X24 del sistema de backup ofertado.
- Registrar y actualizar la evidencia de respaldos y restauraciones en Bitácoras de Backup (Generados automáticamente por la herramienta o en físico), y generar informe mensual de Gestión de backups. Esta bitácora también debe mantener el registro del estado de la plataforma, las acciones sobre la configuración del sistema de backup y el uso de los espacios de almacenamiento.
- Desarrollar un plan de capacidad que incluya una revisión como mínimo una vez al año, donde se evalúe la suficiencia de la infraestructura de respaldos, así como la pertinencia de realizar nuevas adquisiciones o mejoras.
- Apoyar la ejecución de pruebas relacionadas con el servicio de respaldo, solicitadas dentro de los planes de continuidad de negocio y planes de contingencias del INC. Medir y registrar durante estas pruebas los tiempos RTO (Recovery Time Objective) y RPO (Recovery Point Objective), y realizar los ajustes de frecuencia y capacidad sobre los respaldos que se determinen como resultado de estos ejercicios.
- Gestionar el tratamiento y cierre de acciones preventivas, correctivas o de mejora, relacionadas con la plataforma de respaldo.
- Atender solicitudes de creación, eliminación y actualización de políticas de backup.
- Implementar una cadena estricta e integral del proceso de custodia para la gestión de backups, para conservar la integridad y confidencialidad de los respaldos.
- Gestión de alarmas de respaldos en las herramientas de monitoreo, y revisión de los reportes de respaldos.
- Instalar y configurar nuevos clientes y agentes.
- Realizar pruebas periódicas de los respaldos y registrar la evidencia de las mismas.
- Gestionar las garantías y seguimiento de casos con el fabricante del sistema.
- Ejecutar las actualizaciones de versiones y “Hotfix” de las aplicaciones de respaldo.
- Realizar la Migración hacia nuevas versiones de la herramienta de Respaldo.

3.1.10.7. Manejo de residuos de aparatos eléctricos, electrónicos y contaminantes

El contratista deberá encargarse de la disposición final de aparatos eléctricos o electrónicos en el momento en que se descarten de la infraestructura a cargo, así como también los elementos contaminantes que se originen en los empaques de insumos que se desechen, dentro del marco de la gestión integral y cumpliendo los requerimientos de la normatividad vigente. Al inicio del contrato y una vez por cada año de vigencia del mismo, el contratista deberá aportar al Instituto la certificación que acredita que realiza la disposición final como gestor o a través de gestor autorizado, cumpliendo a cabalidad con el manejo ambientalmente adecuado de los residuos de aparatos eléctricos, electrónicos y material contaminante, bajo la normatividad colombiana vigente.

3.1.10.8. Gestión del Cambio

El proceso de cambio en la organización es siempre complejo, pues implica salirse de la zona de confort, generar inconformidades y puede dañar el clima de la organización, sin siquiera hacerse efectivo por los componentes reto, diferencia e incertidumbre. Por ello, se necesita que el contratista realice procesos de gestión del cambio en cuatro frentes claros:

- Diagnóstico del entorno
- Planeación del cambio
- Ejecución del cambio
- Mantenimiento de los cambios

Es por ello que el contratista deberá ejecutar los procesos de gestión del cambio en los que intervenga como ejecutor, y apoyar activamente los procesos de gestión del cambio que impliquen los diversos proyectos de tecnología de la información a implementarse al interior del INC, durante la duración del contrato de Outsourcing.

El contratista será responsable de la documentación de dichos procesos y de la transferencia de conocimiento a los usuarios finales del INC.

4. PROCESO DE INSTALACIÓN Y EMPALME

El plazo estimado para la ejecución del contrato será de 35 meses. Se estiman dos meses iniciales para el proceso de transición y 33 meses para la etapa de operación. Contados a partir de la legalización del contrato y el hasta 30 de abril de 2022.

El Instituto pagará el valor del contrato a los TREINTA (30) días después de radicada factura, previa entrega de los bienes, servicios u obras objeto del mismo, expedición de la certificación de recibo a satisfacción por parte el supervisor o interventor designado por el INC ESE y cumplimiento de los trámites legales, fiscales y administrativos a los que haya lugar. Los pagos se realizarán solamente a partir del inicio de la etapa de operación. Durante la etapa de transición se reconocerán los valores estipulados en el archivo anexo CostosInvitación_outsourcing.xlsx, en la hoja TotalCostos (costos transición – Migración). Los cuales se pagarán por una única vez.

Considerando las características y la complejidad del servicio que se requiere, el contratista deberá iniciar la etapa de transición, una vez firmado el contrato. El nuevo proveedor deberá disponer en sitio del personal para la labor de empalme correspondiente, de acuerdo al cronograma de transición pactado en el acta de inicio.

El proceso de recepción y empalme que realice el contratista, antes del inicio de la operación, no implica facturación para el INC. La facturación para el contratista comenzará con el inicio de la operación de los servicios a su cargo.

El tiempo estimado para la transición y estabilización será de dos (2) meses, contados a partir de la firma del acta de inicio, previa definición del cronograma de entrega e instalación de los equipos de escritorio, tiempo durante el cual el INC pagará los servicios, equipos e insumos al proveedor saliente. En caso de que la transición no se haya logrado en el tiempo estimado, los costos adicionales que impliquen personal de proveedor saliente serán asumidos en su totalidad por el proveedor entrante.

Sólo a partir del inicio de la etapa de operación, el INC iniciará el pago del servicio correspondiente, previa verificación y certificación por parte de los supervisores técnicos del contrato, aclarando que equipo o servicio que no se encuentre en producción, no se pagará.

El contratista entrante deberá realizar los procesos de recepción, empalme, operación y entrega de la plataforma tecnológica e informática, servicios, inventarios, documentación, contraseñas y demás elementos y componentes inherentes al objeto del contrato, en los tiempos acordados con la supervisión del contrato, previo plan y cronograma de actividades.

Durante la etapa de empalme se deberán realizar pruebas exhaustivas que garanticen la operatividad del servicio bajo la nueva plataforma y se verifique la correcta integración de los procesos de negocio actuales del INC, lo cual incluye control total de la seguridad informática, redes, impresión, servicio de correo, servicio de mesa de ayuda, administración de canales dedicados, sistema de gestión y monitoreo general, entrega formal de inventarios, entre otros.

Como resultado de esta etapa de empalme, pruebas y verificación se obtendrá actas de prueba de aceptación por cada equipo o servicio que harán parte de un documento entregable firmado entre las partes sobre el cual se dará autorización para entrar en producción con el total de la solución

En la firma del acta de inicio se debe hacer entrega de un cronograma de instalación que detalle las actividades de implementación a realizar, identificando responsable y recursos involucrados, de forma tal que se garantice la entrada en producción en la fecha esperada.

Una vez finalizado el contrato que se derive de la presente invitación y sus posibles adiciones futuras el contratista deberá garantizar un periodo de empalme o transición con el nuevo proveedor mínimo de 2 meses y se pagara a las tarifas acordadas del último mes contra la liquidación del contrato.

Dentro del desarrollo y ejecución del contrato que se derive de la presente invitación el INC podrá excluir los servicios que estime convenientes, previo aviso con una antelación de 60 días.

4.1. Etapa de transición inicial

La Etapa o Periodo de Transición corresponde al periodo durante el cual el Contratista planea, aprovisiona, e instala la infraestructura base para el inicio de la prestación de los servicios a la Entidad. Durante dicha etapa implantará el Modelo de Prestación de Servicio, los procedimientos y tecnologías que permitan el control y la estabilización de los servicios. De igual manera, establecerá los protocolos y formatos con la Entidad para lo que será la prestación del servicio durante el resto de la ejecución del contrato y habrá realizado la alimentación de los procesos ITIL oficiales requeridos por la entidad en la Herramienta de Gestión.

La etapa de transición tendrá una duración estimada de dos (2) meses, contados a partir de la fecha de la firma del Acta de Inicio del Contrato, misma que debe suscribirse a más tardar a los 3 días hábiles siguientes a la suscripción del Contrato.

El Instituto pagara los productos y servicios que durante esta etapa sean implementados o entregados por parte del proveedor entrante, y que sean liberados por el proveedor saliente. Estos productos y servicios serán liquidados, conforme a las tarifas pactadas. Para esto en la Hoja TotalCostos, Ítem 9 Costo Transición Anticipada, del documento Anexo No. 8 CostosInvitacionPublica_Outsourcing.xlsx, se dispone de un presupuesto de hasta cien millones de pesos ($100.000.000), IVA incluido.

4.1.1.1. Actividades a ejecutar durante la etapa de Transición - Migración

Desde el inicio del contrato el Contratista realizará el despliegue del personal en el Instituto conforme al plan de transición acordado entre las partes.

En esta etapa de transición, el contratista entrante deberá liderar el proceso de transición, garantizando la continuidad operativa de todos los servicios que presta el contratista saliente al INC.

El contratista deberá disponer del personal suficiente y necesario para la etapa de transición y empalme, sin que esto afecte la prestación normal de los servicios. El personal dedicado a la transición deberá tener una disponibilidad 7x24.

El contratista debe garantizar la logística de suministro, instalación e implementación de todos los equipos y servicios. Lo anterior incluirá una planeación de la instalación de equipos que no implique volúmenes grandes de almacenamiento dentro del INC, dado que no cuenta con áreas de bodegaje.

Al inicio del contrato, el Contratista presentará un documento que contenga el Modelo de Prestación del Servicio de mesa de ayuda al INC. El modelo de prestación de servicios debe estar alineado a las prácticas de ITIL V3, para la operación del servicio.

Estos documentos serán revisados por la Supervisión del Contrato, y el Contratista deberá hacer los ajustes que le sean solicitados o sugeridos.

Además, durante esta etapa el Contratista adelantará las actividades necesarias para el control y estabilización de los servicios contratados. Las actividades durante esta etapa corresponden, pero no se limitan a:

- Implantación e implementación de la Herramienta de Gestión, con procedimientos básicos de atención.
- Montaje y configuración de los ANS sobre la Herramienta de Gestión de la mesa de servicio, durante el primer mes de ejecución del contrato.
- Presentación del Plan mediante la cual desarrollará la Etapa de Transición, incluyendo el reemplazo de los elementos de continuidad que tenga instalados el prestador anterior del servicio de mesa de ayuda.
- Entrega de publicidad y campaña de gestión del cambio en los sitios dentro del alcance de la mesa de ayuda.

Para el cumplimiento de los fines de la etapa de transición, el Contratista presentará planes detallados para desarrollar cada uno de los siguientes aspectos:

- Definición del Servicio: debe indicar como llevará a cabo.
- Implantación del Modelo de Prestación de Servicios
- Transición y empalme de los servicios (transferencia de procesos operativos y de conocimiento).
- Formalización de los ANS - incluye definición de indicadores de servicio, establecimiento de indicadores de servicio, niveles de rendimiento, Nivel de servicio Objetivo NSO, Niveles de servicio mínimos NSM, métrica del servicio, indicadores, procedimientos de medición y monitoreo, reportes de gestión y documentación.
- Los indicadores NSO y NSM iniciales, que se deben cumplir por parte del Contratista en la prestación de los servicios, para la Mesa de Ayuda se consignan en el documento Anexo_NivelesdeServicio.xlsx.
- Estos indicadores podrán ser actualizados periódicamente y de común acuerdo entre la Entidad y el Contratista, de conformidad con un análisis previo en materia de arquitectura tecnológica y oportunidades de mejoramiento disponibles.
- Plan de comunicaciones Internas: definir cómo se llevará a cabo la divulgación de los procesos y condiciones del servicio.
- Plan de mitigación del riesgo: programa que asegure la continuidad de los servicios contratados y la identificación y contención de los posibles riesgos asociados con la implantación y estabilización del Modelo de Prestación del Servicio.

Dentro de las actividades a desarrollar a manera global están:

Tabla 21: Actividades Generales de Transición

Periodo de transición
Planeación
Servicios de Directorio activo, Dominio y servidores
Implementación Servidores
Gestión de Servidores
Implementación Servidores Outsourcing
Equipos de cómputo e Impresoras
Instalación de equipos de usuario final e Impresoras
Migración Office 365
Fase 1: Verificación y optimización de Redes y canales
Fase 2: Definición de Identidad y autenticación de usuarios
Fase 3: Instalación de Office 365 Pro Plus en equipos de usuario final
Fase 4: Migración de Correo Zimbra e implementación de Exchange Online
Fase 5: Activación e implementación de OneDrive 1TB x usuario.
Fase 6: Aplicación de controles de seguridad y protección de la información
Fase 7: Administración de dispositivos móviles
Fase 8: Capacitación y Gestión del cambio a todos los usuarios de Office 365
Servicios de Seguridad
Migración de UTM
Implementación Arquitectura de Red Recomendada
Configuración Servicios Básicos Firewall Nueva Generación
Montaje Servidores VM Antispam en HA
Integración y configuración servicios Antispam
Implementación Plataforma Backups
Instalación Consola de Antivirus
Implementación Antivirus
Implementación DLP Office 365
Configuración Servicios Avanzados Firewall Nueva Generación
Implementación DLP Endpoint
Instalación y configuración servicio de monitoreo
Servicios de Red

Recepción de administración de RED Alámbrica, Inalámbrica y Conectividad
Recepción Centros de Cableado
Instalación UPS centros de cableado
Administración red
Migración VLANS Firewall Nueva Generación
Instalación y configuración servicio de monitoreo
Mesa de ayuda y soporte
Recepción Mesa de soporte
Instalación y configuración de Aplicativo Mesa de ayuda e inventarios
Inicio de nuevo soporte
Fin Transición

Además de todas las actividades adicionales que sean necesarias para el proceso de transición.

Para cada uno de los aspectos, durante la fase de planeación, se deberán entregar los planes propuestos deben relacionar como mínimo:

- Descripción general.
- Plan y cronograma detallado (actividades, recursos, duración, productos).
- Roles y Responsabilidades de las partes
- Criterios de aceptación y Listas de Chequeo.

4.2. Etapa Operación

La etapa de operación comprende el periodo desde la finalización de la etapa de transición hasta la finalización del contrato.

Los casos no solucionados ni cerrados (incidentes y requerimientos) que pasen de la etapa de transición a la etapa de desarrollo empezarán a ser objeto de evaluación de ANS, para lo que se considerará como fecha inicial y hora inicial de cada caso el día de inicio de la etapa de desarrollo, a las 0:00 horas.

El Contratista debe presentar el costo total que integra la ejecución del contrato, de igual manera el costo mensual, y su totalización al final de los treinta y cinco (35) meses, (etapa de transición + etapa de operación), de acuerdo con el **Anexo No. 8 CostosInvitacionPublica_Outsourcing.xlsx.**

La formulación del Costo total deberá considerar que el alcance y las condiciones técnicas de la prestación de los servicios presentadas en la propuesta base, se mantienen invariables durante la ejecución del contrato. Es por cuenta del Contratista, compilar y analizar la información que estime pertinente para efectos de proponer dicho costo durante el proceso de selección.

Con la presentación de su propuesta, el Contratista entiende y acepta que el costo total propuesto es el valor máximo que pagará el INC durante la ejecución del contrato, como pago por la prestación de los servicios, bajo las condiciones y cobertura de los mismos consignados en los **Anexo No. 7 TecnicosInvitacionPublica_Outsourcing.xlsx y Anexo No. 8 CostosInvitacionPublica_Outsourcing.xlsx.**

Se advierte que, en el evento en que el INC no modifique las condiciones de la prestación de los servicios establecidos en los Acuerdos de Niveles de Servicio, o la demanda del servicio y el Contratista desarrolle las actividades a su cargo de tal manera que los costos del servicio sean mayores al costo total que él definió en su propuesta, el valor adicional correrá por cuenta del Contratista, sin que en tal caso haya lugar a reconocimiento económico alguno por parte del INC.

Si la Entidad considera necesario reajustar los términos y condiciones pactados en el contrato, los ajustes se realizarán de mutuo acuerdo con el contratista, cuando las causales de los ajustes sean:

- Requerimientos o modificaciones a los ANS
- Cambios imprevistos de la plataforma tecnológica
- Ajustes significativos de la demanda de servicio
- Aprovechamiento de oportunidades de mejoramiento

- Por otras razones que, a juicio del INC, ameriten los reajustes mencionados.

4.3. Etapa de empalme final

Una vez finalizado el contrato que se derive de la presente invitación y sus posibles adiciones futuras el contratista deberá garantizar un periodo de empalme o transición con el nuevo proveedor mínimo de 2 meses y se pagaran a las tarifas acordadas del último mes contra la liquidación del contrato.

Durante los dos (2) últimos meses de la etapa de operación, se surtirá el empalme con el INC, o el nuevo Contratista del servicio de mesa de ayuda (si existe).

Durante estos dos (2) últimos meses, el Contratista deberá prestar al INC los servicios objeto del contrato, hasta el momento en que el INC o un tercero designado por la misma, esté en capacidad de asumir la responsabilidad en la prestación de los servicios, sin que por ello se vea perjudicada la continuidad de la prestación de los servicios informáticos al INC.

Este proceso tendrá las siguientes actividades:

- Planes de prueba y aceptación de componentes de infraestructura del INC conformada por los Servidores, equipos de cómputo, portátiles, Impresoras, Equipos activos de red, UPS y Reguladores, entre otros, verificando que se encuentren operativos y en normal funcionamiento. Las excepciones deben estar registradas en la base de datos de la herramienta de gestión, donde se encuentran los casos asociados y la razón de su no cierre. Se debe entregar la relación de dichos casos.
- Documentación de los ANS, bases de datos de incidentes, requerimientos, problemas y configuraciones: se adjunta la información de la base de datos de la herramienta de gestión, la cual contiene el registro de todos los casos generados. Cada uno de los casos tiene asociado un único número de servicio, el status al momento de la exportación a Excel de la base de datos y describe todo el historial de dicho servicio desde su generación hasta su cierre o status actual. Se incluye igualmente la Base de Datos de usuarios vigente en formato Excel, el consolidado de los equipos de soporte del Contrato y la relación de dichos equipos instalados.
- Documentación de aspectos de seguridad (arquitecturas, usuarios, contraseñas, procedimientos): se adjunta el archivo contenido en un CD, con la relación de claves de seguridad (usuarios y contraseñas) suministrada para ser utilizadas en la operación, así como el procedimiento para la cual fue utilizada, usuarios y contraseñas de servidores y servicios que se deban administrar. Estructura VLAN, inventario de IP fijas, relación de IP reservadas, topologías LAN y WAN, Direccionamiento IP, Direccionamiento de red, máscaras, *broadcast* y tipo de conexión, VPNS, solución antispam de correo electrónico, sistema de analítica de eventos y amenazas, políticas y reglas aplicadas, entre otros.
- Entrega de listas de chequeo del mantenimiento preventivo de UPS, Reguladores, Redes de datos y eléctricas reguladas, inventarios de puntos de datos y eléctricos regulados, inventario de equipos activos, diagramas unifilares y diagramas de red local, entre otros, de las seccionales cubiertas por el contrato.
- Presentación en medio digital de los mantenimientos preventivos de PCs, impresoras, escáner, etc.
- Relación de inventario de Hardware/Software: con la información de la base de datos de la herramienta la cual contiene el registro del inventario de Hardware y Software de la plataforma tecnológica del INC en formato Excel además un folder con actas (CD CMDB actualizada).
- Equipos en garantía con seriales, fecha de vencimiento, proveedor, datos de proveedores actuales para trámite de garantías.
- Contraseñas de Seguridad tipo Endpoint, consola antivirus actual, información general del antivirus, reglas del antivirus Contraseñas, exclusiones de antivirus, reglas y configuraciones DLP Endpoint, reglas y configuraciones DLP Endpoint de correo electrónico.
- Informe con el estado actual de la herramienta de monitoreo. (Informe actualizado del monitoreo de servidores y equipos activos de red).
- Estado actual de WSUS, que tiene implementada la consola y estado actual. Contraseñas de WSUS de acceso a la consola.
- Documentación técnica y en general toda la información que facilite la prestación de los servicios por parte del INC o de un tercero diferente al Contratista.
- Se entrega la Base de Datos de la Herramienta de Gestión en formato nativo y en formato Excel.

5. PROYECTOS DE GESTIÓN TECNOLÓGICA

Durante la duración del contrato, el INC ejecutará diversos proyectos de gestión tecnológica, para los cuales se necesitará el acompañamiento del Outsourcing de servicios TI, que incluyen, pero no se limitan a los siguientes:

5.1. Transición a IPV6 (resolución 2710 de 2017)

Dado que el Instituto para el segundo semestre de 2019, implementara un proyecto que tendrá como misión la transición a IPv6, para cumplir con la Resolución 2710 de 2017 del Ministerio de Tecnologías de la Información y las Telecomunicaciones – Min Tic, y la normatividad que la modifique o sustituya. El contratista seleccionado, deberá participar de la transición, prestando su apoyo a las actividades relacionadas con dicho proyecto, dado su rol de administrador de la red y de seguridad informática.

5.2. Proyecto de actualización de Redes

El Instituto para el segundo semestre de 2019 ejecutará un proyecto de consolidación y modernización de los servicios de redes de voz y datos, por lo que el contratista seleccionado deberá apoyar deberá participar de la transición, prestando su apoyo a las actividades relacionadas con dicho proyecto, dado su rol de administrador de la red.

5.3. Proyecto Plan de continuidad de Negocio

El Instituto para el segundo semestre de 2019 y primer semestre de 2020 ejecutara un proyecto de consolidación de su plan de continuidad de negocio por lo que se requiere que el contratista seleccionado participe en la ejecución de las pruebas y solución de planes de acción propuestos, dado su rol de administrador de la red y seguridad informática.

6. ANEXOS

6.1. Descripción de las hojas del archivo Excel: Anexo No. 7 TecnicosInvitacionPublica_Outsourcing.xlsx

En la siguiente tabla se describe cada una de las hojas Archivo Excel Anexo No. 7 TecnicosInvitacionPublica_Outsourcing.xlsx el cual hace parte de la invitación y debe ser diligencia de forma obligatoria de la forma como se indica, debe ser entregada de forma impresa y en medio magnética en el mismo formato Excel.

Tabla 22: Descripción de las hojas del Archivo Excel Anexo No. 7 TecnicosInvitacionPublica_Outsourcing.xlsx

ARCHIVO EXCEL ANEXO No. 7 TECNICOSINVITACIONPUBLICA_OUTSOURCING.XLSX		
Nombre de la Hoja	**Descripción**	**Diligenciar por parte del oferente**
EMR	Especificaciones Mínima requeridas de Hardware	SI
Anexos Admin	Equipos administrados	NO
Licenciamiento	Información de Licenciamiento	NO
Talento Humano	Evaluación Talento Humano	SI
ProductosContingencia	Cantidad de equipos de contingencia requeridos	NO
Experiencia	Experiencia del proponente	SI
Certificaciones	Certificaciones del proponente	SI
RTG	Requerimientos Técnicos Generales	SI

6.2. Descripción de las hojas del archivo Excel: Anexo No. 8 Costosinvitacionpublica_outsourcing.xlsx

En la siguiente tabla se describe cada una de las hojas Archivo Excel Anexo No. 8 CostosInvitacionPublica_Outsourcing.xlsx el cual hace parte de la invitación y debe ser diligencia de forma obligatoria de la forma como se indica, debe ser entregada de forma impresa y en medio magnética en el mismo formato Excel.

Tabla 23 Descripción de las hojas del Archivo Excel Anexo No. 8 CostosInvitacionPublica_Outsourcing.xlsx

ARCHIVO EXCEL ANEXO No. 8 COSTOSINVITACIONPUBLICA_OUTSOURCING.XLSX		
Nombre de la Hoja	**Descripción**	**Diligenciar por parte del oferente**
CostoProductosServicio	Productos Servicios y costos de la oferta detallados	SI
OtrosCostos	Otros costos relacionados con la operación	SI
CostoMigracion	Otros costos relacionados con la Migración Y Gestión del Cambio	SI
TotalCostos	Ficha resumen costos	SI

7. Índice de Tablas