



MINISTERIO DE VIVIENDA, CIUDAD Y TERRITORIO

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

ANEXO TECNICO N. 3

NOC y SOC Fase II

2026

Tabla de contenido

1.	INTRODUCCION	3
2.	SERVICIOS POR PROVEER	3
2.1.	CONECTIVIDAD.....	3
2.2.	DATACENTER.....	4
2.2.1.	SUMINISTRO DE CAPACIDADES DE COMPUTO	4
2.2.2.	SERVICIO DE BASE DE DATOS ORACLE	4
2.2.3.	SERVICIOS DE NUBE	5
2.3.	GESTION DE INFRAESTRUCTURA.....	5
2.4.	GESTION DE ALMACENAMIENTO Y COPIAS DE SEGURIDAD	6
2.5.	GESTION DE SERVICIOS, APLICACIONES Y BASES DE DATOS	6
2.6.	GESTION DE REDES	10
2.7.	SERVICIO DE OPERACIONES DE SEGURIDAD DE LA INFORMACION (SOC).....	11
2.7.1.	GENERALIDADES	11
2.7.3.	SERVICIO DE OPERACIONES DE SEGURIDAD PERIMETRAL.....	13
2.7.4.	ACTIVIDADES ESPECÍFICAS DEL SOC	14
2.9.	MONITOREO DE LA SOLUCION OFERTADA	15
2.10.	REPORTES	16
2.11.	TABLEROS DE GESTIÓN	17
2.12.	DRP.....	17
2.12.1.	GENERALIDADES	18
2.12.2.	CONDICIONES DEL SERVICIO	18
2.12.3.	REQUISITOS ESPECIFICOS DE LA SOLUCION.....	19
3.	OTROS SERVICIOS	23
3.1.	ESPACIO EN RACK EN DATA CENTER.....	¡Error! Marcador no definido.
3.2.	CUSTODIA DE MEDIOS	23
3.3.	AMPLIACION RENOVACION DE LICENCIAMIENTO APLICACIONES.....	¡Error! Marcador no definido.
4.	MIGRACION Y TRANSICION	¡Error! Marcador no definido.
5.	DOCUMENTOS RELACIONADOS	24

1. INTRODUCCION

En el presente Anexo Técnico se presenta una descripción detallada para la operación del servicio de Centro de Datos en modalidad híbrida el cual contempla:

Los servicios de conectividad, centro de datos, infraestructura como servicio, nube privada, hosting y nube pública con el fin de suplir las necesidades de gestión de infraestructura de TIC, gestión de información, gestión de componentes tecnológicos y sistemas de información del Ministerio de Vivienda Ciudad y Territorio.

2. SERVICIOS POR PROVEER

Las siguientes son las líneas de servicios requeridas para la operación de los servicios del Ministerio de Vivienda, Ciudad y Territorio.

2.1. CONECTIVIDAD

Se requiere que el proveedor opere dentro de su solución el servicio de conectividad entre sedes del Ministerio de Vivienda, Ciudad y Territorio y servicio de internet descentralizado, como una solución de SD-WAN con una capa de seguridad de filtrado de paquetes tipo firewall en cada sede, de acuerdo con las cantidades relacionadas y detalladas en el cuadro presentado a continuación.

Sede	MPLS (Mbps)	Internet (Mbps)	Tipo
Centro Colseguros Bogotá	400	600	SD-WAN
Palma Real Carrera 13 # 28-01 Bogotá	200	200	SD-WAN
La Fragua Calle 17 sur # 30-04 Bogotá	50	50	SD-WAN
Botica Carrera 6 # 8-72 Bogotá	200	500	SD-WAN
Centro de Datos del Proveedor	500	500	SD-WAN
Nube Publica AWS – Centro de Datos	200		

Obligaciones:

- La prestación del servicio se debe estimar hasta el 31 de diciembre de 2026.
- La solución debe permitir alcanzar una disponibilidad del 99.98%.
- Las necesidades de la entidad son lo que se plasman en los anexos de la Fase I, cualquier cambio en los requerimientos técnicos solicitados en estas fichas técnicas, serán los que la entidad requiere en este momento, por tanto, cualquier cambio que se realice posteriormente, será objeto de verificación jurídico técnico.

d. Se debe considerar que la sede principal puede cambiar de ubicación en la misma ciudad.

EL PROVEEDOR deberá garantizar la correcta operación, administración y monitoreo de las Herramientas de Monitoreo y/o Gestión necesarias para la medición y monitoreo del servicio y certificar la no manipulación de los resultados, el acceso, la verificación y validación de estos.

El MVCT cuenta con bloque /48 y plan de direccionamiento propio de IPV6 y el proveedor debe incluir la renovación de la membresía por los periodos que dure el servicio y garantizar que todos los servicios operen sobre IPV6, teniendo en cuenta que toda la infraestructura actual del MVCT funciona en doble stack IPV4/IPV6.

2.2. DATACENTER

Para este servicio se consideran dos ubicaciones al menos. Una ubicación en un Datacenter local, al cual se hace referencia como nube privada y una ubicación en nube pública.

Para la nube pública se establecerá una bolsa de dinero fija por vigencia, para alojar la cantidad de cargas equivalentes a ese valor. El proveedor debe realizar la identificación de las nuevas cargas candidatas y realizar la migración de estas, sin exceder este valor de bolsa definido. El proveedor utilizará las herramientas de las nubes públicas para mantener estos valores y realizar actividades de mejora en eficiencia y costo y las demás definidas en el modelo de Gobierno de las nubes privada y pública propuesto por el proveedor.

Para los servicios de nube privada, el proveedor deberá operar en un centro de datos con características mínimo TIER III o equivalente tanto en diseño como en construcción y estar ubicado en la ciudad de Bogotá o en Cundinamarca, este debe ser de propiedad del ISP o del proveedor de servicios; así mismo, deberá garantizar que la certificación del Datacenter se mantenga vigente. Adicionalmente el DC debe contar con las siguientes certificaciones: ISO 9001:2015, ISO 27001:2022 e ISO 20000-1:2018.

2.2.1. SUMINISTRO DE CAPACIDADES DE COMPUTO

La entidad actualmente tiene sus cargas de trabajo de cómputo virtualizada (máquinas virtuales), el proveedor deberá garantizar la continuidad de la operación de esta plataforma virtualizada en su granja de servidores de nube privada manteniendo el reuso establecido en la fase de transición – migración.

SERVICIO DE BASE DE DATOS ORACLE

El proveedor debe proveer la infraestructura necesaria para cumplir con las restricciones de licenciamiento de acuerdo con las licencias establecidas en la línea base de la fase I.

El proveedor podrá ofrecer en cualquier momento de la operación servicio alternativo para hospedar el motor de base de datos Oracle, siempre y cuando cumpla los requerimientos de licenciamiento y entregue un desempeño igual o superior al actual:

Marca	Referencia	Tipo	Version CPU	Familia CPUs	CPUxCores	CoresTotal	Memoria	Descripcion
Cisco UCS 5108 (FOX1736GP9P)	UCSB200M3	Servidor	E5	2600 v2 @3.0Ghz	2x4	8	192	Servidor Cisco UCS (Oracle)
Cisco UCS 5108 (FOX1736GP9P)	UCSB200M3	Servidor	E5	2600 v2 @3.0Ghz	2x4	8	192	Servidor Cisco UCS (Oracle)

2.2.2. SERVICIOS DE NUBE

Estos servicios, deben incluir todos los elementos y condiciones de la arquitectura, especificados en este anexo técnico (que apliquen al modelo de servicio en nube híbrida), incluyendo la administración de la línea base y la gestión con los proveedores. Se debe ajustar el modelo actual de Gobierno de nube, que permita controlar y optimizar los costos y que el proveedor implementará generando reportes periódicos de uso y la aplicación de herramientas disponibles en la nube pública que apoyen el Gobierno.

El proveedor del servicio entregará, los planes de contingencia de los servicios y el plan de continuidad del servicio del Datacenter, en donde se puedan identificar las diferentes estrategias consideradas para brindar la continuidad de los servicios, plan de comunicaciones con el cliente, acciones específicas cuando el servicio va a estar más de 12 horas por fuera y plan de restablecimiento del servicio. Se debe incluir la matriz de escalamiento y la remediación del servicio.

El proveedor entregará y mantendrá actualizado al MVCT las arquitecturas de las ubicaciones donde se alojarán los servicios, incluyendo los controles de acceso, la seguridad perimetral y las medidas de ciberseguridad.

El proveedor convocará una sesión de trabajo cada dos meses para revisar los sistemas o aplicaciones a ser migrados entre los servicios de nube, teniendo en cuenta la capacidad de la bolsa de dinero establecida para los servicios de nube pública.

2.3. GESTION DE INFRAESTRUCTURA

El proveedor deberá operare un servicio que incluya la administración de toda la línea base contemplada en los anexos que hacen parte del servicio, para lo cual deberá disponer de infraestructura de hardware y software suficiente para alojar los ambientes de producción, prueba, desarrollo y el cluster de openshift, de acuerdo como se definieron en la fase de transición – migración.

Para la operación se requiere que los ambientes de virtualización estén separados en arreglos de servidores físicos independientes, para ambiente de producción se requiere como mínimo un arreglo de tres máquinas físicas, para el cluster de openshift mínimo dos máquinas físicas y para los ambientes de pruebas-desarrollo mínimo dos máquinas.

2.4. GESTION DE ALMACENAMIENTO Y COPIAS DE SEGURIDAD

El proveedor debe garantizar la continuidad del servicio de Backup actual con capacidad de 100TB. Debe implementar un servicio que permita realizar restauración granular de la información. Actualmente los respaldos son realizados con Veeambackup que se tienen en el marco de la fase I de transición – Migración.

El Almacenamiento en calidad de servicio de 180 TB efectivos se debe garantizarse durante toda la etapa de operación que están presentados a los clusters de VMware, así mismo, el proveedor deberá realizar los Incrementos de capacidad de almacenamiento en la infraestructura virtual, de acuerdo con las estadísticas de crecimiento de las BD o File System, con las capacidades disponibles de la línea base que se asignarán a los Sistemas de Información y plataformas de acuerdo con los requerimientos de la fase I de transición-migración.

El proveedor deberá realizar pruebas de restauración de forma periódica (mensualmente a 2 sistemas de información) en un ambiente controlado, que permita validar la integridad de los datos y restauración, el cual se debe incluir en el informe mensual para ser validadas por el MVCT.

2.5. GESTION DE SERVICIOS, APLICACIONES Y BASES DE DATOS

Para garantizar la disponibilidad y acceso permanente de la información que los usuarios usan para llevar a cabo sus actividades, se requiere que el proveedor entregue dentro de su solución el servicio de administración, operación y soporte técnico con fabricante de, aplicaciones, plataformas, servicios y bases de datos de la infraestructura TI del MVCT incluidas en el **Anexo 1 Líneas Base (no aplica para software libre)**, junto con sus servicios, y componentes.

Las actividades a llevar cabo dentro de la administración son definidas por las guías y mejores prácticas en administración de tecnología definidas por el proveedor y acordadas con el MVCT y en ellas se deben incluir las siguientes **tareas**, para **todos** los componentes administrados incluidos en la **Línea Base** (Sistemas Operativos, Bases de datos, máquinas virtuales, etc.):

1. Administrar y monitorear 7X24X365 la operación de la infraestructura de hardware y software que soporta los servicios tecnológicos del MVCT, e informar a la entidad, sobre cualquier evento o incidente que se presente.
2. Atender requerimientos fines de semana y en tiempo fuera de horario laboral del MVCT, en caso de que se requiera.
3. Ejecutar paradas, subidas y reinicios de servicios, aplicaciones, plataformas, incluidos en la línea base.
4. Verificar la salud de los componentes de la plataforma administrada usando bitácoras de revisión y/o herramientas de monitoreo.
5. Asegurar la operación adecuada de todos los componentes de la plataforma administrada.
6. Identificar necesidades de afinamiento en los componentes administrados, documentar los resultados esperados y aplicar los ajustes y/o configuraciones requeridas siguiendo el procedimiento de control de cambios.
7. Realizar un aseguramiento trimestral preferiblemente con los fabricantes o con un experto de cada plataforma para seguridad perimetral (firewall, waf, etc.), endpoints de la entidad (portátiles, equipos de escritorio, impresoras, móviles, etc.) y cuentas de usuario y servicio, e información en tránsito y reposo.
8. En caso de falla de algún componente de la plataforma administrada llevar a cabo el proceso de solución de fallas (troubleshooting), que debe contemplar la identificación de la falla, creación de caso de falla en la herramienta de atención de requerimientos y de acuerdo con el impacto, generar comunicación y escalamiento con el proveedor.
9. Monitorear y actualizar el estado de los tickets en la herramienta de gestión de incidentes, incluyendo la documentación de las actividades realizadas hasta que el ticket quede en estado cerrado/resuelto. Tras la ocurrencia del incidente el proveedor debe entregar en máximo 2 días hábiles después de ocurrida la incidencia un informe causa raíz con el detalle completo de la misma teniendo en cuenta los procedimientos y formatos establecidos en el Sistema de Gestión de Calidad y de igual forma en el informe de gestión mensual y seguimiento, debe presentarse la relación de incidencias. Así mismo, este informe debe contener el plan de remediación y se debe atender las observaciones y requerimientos que se establezcan por parte del Oficial de Seguridad de la Información y el Supervisor.
10. Aplicar metodologías para resolución rápida y estructurada de incidentes, teniendo en cuenta los procedimientos definidos por el MVCT.
11. Cumplir con el procedimiento de Control de Cambios definido con el MVCT.
12. Definir en conjunto con el MVCT las políticas de Backup requeridas para garantizar la continuidad de la información de acuerdo con su importancia en la entidad.
13. Asegurar la toma de Backups de acuerdo con las políticas definidas, enviando el reporte diario con el estado exitoso y fallido a la Supervisión.
14. Asegurar la actualización de los componentes de la plataforma administrada, incluyendo parches, fixes y demás liberados por el fabricante. En el caso que una actualización genere impacto en las aplicaciones o servicios se debe llevar a cabo una reunión de entendimiento

- y alerta con el responsable del servicio del MVCT e identificar los posibles riesgos y la forma de mitigarlos.
15. Acordar con el MVCT el cronograma de aplicación de parches diferenciados por cada ambiente.
 16. Aplicar las mejores prácticas y recomendaciones en aplicación de parches para garantizar el éxito en la actividad y la continuidad del servicio.
 17. Entregar el procedimiento al MVCT de aplicación de parches.
 18. Definir con el MVCT la política de aplicación de parches.
 19. Garantizar la aplicación de plantillas de seguridad y prácticas de aseguramiento definidas en conjunto.
 20. Llevar el registro de fallas, problemas, soluciones, acciones desarrolladas, solicitudes adicionales de respaldo, restauraciones, trabajos realizados y en general todos los detalles de la operación en la herramienta de gestión, el cual deberá ser presentado a través de un tablero de control que tenga acceso la Entidad.
 21. Recopilar, construir y mantener actualizado los Mapas e inventario de los sistemas de información y componentes tecnológicos alojados en el centro de datos del proveedor.
 22. Llevar un control estricto de las operaciones y acciones realizadas sobre los aplicativos a fin de cumplir con los ANS definidos; se deben generar informes mensuales con las recomendaciones y/o escalamientos generados a las áreas de desarrollo.
 23. Identificar, notificar y proponer planes de mitigación a posibles riesgos de seguridad en la operación, cambios de datos o pasos a producción (Utilización de usuarios privilegiados, usuarios o direcciones IP quemados en el código, implementación de prácticas no recomendadas en los aplicativos, puntos únicos de fallas, entre otros).
 24. Escalar al soporte del siguiente nivel en caso de que se requiera. Si el escalamiento es con canal autorizado, vendedor, fabricante, etc. El proveedor es el responsable de gestionar el caso (creación, documentación, solicitud de estados de avance, solicitud de escalamiento adicional, cierre a conformidad).
 25. Gestionar las cuentas de usuarios en los componentes administrados.
 26. Participar por demanda en reuniones de nuevos proyectos que impacten los componentes descritos en la línea base, el cual deberá actualizar esa misma línea base.
 27. Acompañar durante las definiciones de uso, despliegue de nuevos sistemas, servicios y aplicaciones que afecten los componentes descritos en la línea base.
 28. Acordar con el MVCT los requerimientos de reportes de capacidad y desempeño requeridos.
 29. Generar reportes de capacidad y desempeño de acuerdo con los procesos y procedimientos definidos con el MVCT.
 30. Generar informes por plataforma detallada en la línea base, en el que se incluya el uso, incidentes, recomendaciones y planes de mejora.
 31. Elaborar el plan de administración por cada plataforma administrada detallada en la línea base.
 32. Generar un reporte mensual de la aplicación de parches y actualizaciones.

33. El proveedor deberá realizar la gestión de usuarios de las plataformas como servicio que tiene la Entidad (Office 365, IfindIT, entre otras) durante la ejecución del contrato.
34. El proveedor deberá cumplir con todas las políticas y lineamientos de la Entidad incluyendo la de seguridad y privacidad de la información definidos en el manual de políticas de seguridad y privacidad de la información y seguridad digital del ministerio de vivienda, ciudad y territorio (Anexo).
35. Actualizar con colaboración del MVCT, la matriz de activos de información con los que cuenta la entidad.
36. Administrar la gestión de los riesgos digitales y de ciberseguridad de acuerdo con la metodología establecida en la norma ISO 31000 / ISO 27005 o la que el proveedor maneje que cumplan con los lineamientos dados por el Gobierno Nacional.
37. Cumplir con la normatividad de la Guía 12 – Seguridad en la Nube, establecida por el Ministerio TIC, en el cual se presentan los lineamientos y aspectos para tener en cuenta para el aseguramiento de la información en la nube – Cloud; en las Entidades del Estado.

Actividades Específicas en Bases de Datos

Adicional a las actividades anteriores para bases de datos se deben realizar las siguientes:

- Ejecutar el proceso de despliegue de componentes de bases de datos, scripts, sp, sqls, etc.
- Ejecutar la rotación y la custodia de los logs de los motores de bases de datos de acuerdo con la propuesta del proveedor previa aprobación del supervisor del contrato.
- Apoyar a los demás equipos de administración del contexto tecnológico del MVCT, en la resolución de incidentes que afecten la disponibilidad de servicios y aplicaciones.
- Ejecutar la recuperación desde backup de archivos, sistemas operativos y datos de Motores de bases de datos que se encuentran en la línea base.
- Construir, desplegar y monitorear ETLs de acuerdo con las necesidades de la entidad.
- Crear vistas materializadas o indexadas de acuerdo con las necesidades de la entidad.
- Crear instancias de bases de datos requeridos para ambientes no productivos y productivos requeridos por las necesidades de operación de las áreas.
- Ajustar y mantener actualizada la línea base.
- Elaborar el plan de administración incluyendo las actualizaciones de los motores de base de datos.
- Identificar mejoras en la operación de base de datos y participar en la implementación de mejoras.
- Realizar despliegues, ajustes de vistas y mantenimiento a los datos en la bodega de datos.
- Mantener actualizados los diccionarios de Datos.
- Participar en la definición y aplicación de los estándares de Datos.

Actividades Específicas en Middleware y Aplicaciones

Adicional a las actividades anteriores para el Middleware y las aplicaciones se deben realizar las siguientes:

- Ejecutar el proceso de despliegue de aplicaciones.
- Ejecutar la rotación y la custodia de los logs de los productos Middleware de acuerdo con la propuesta del proveedor, previa aprobación del supervisor del contrato.
- Apoyar a los demás equipos de administración en la resolución de incidentes que afecten la disponibilidad de servicios y aplicaciones.
- Ejecutar la recuperación desde backup de archivos y productos de aplicaciones y Middleware que se encuentran en la línea base.
- Mantener los documentos actualizados con la operación y la administración de la plataforma de aplicaciones y Middleware.
- Administrar los certificados SSL y llaves que se encuentran configurados en los servidores de aplicaciones y Middleware de la línea base.
- El proveedor deberá realizar las automatizaciones o mejoras en los flujos de procesos de las herramientas de Mesa de Servicio y Office 365.
- Ajustar y mantener actualizada la línea base.
- Elaborar el plan de administración incluyendo las actualizaciones del middleware y las aplicaciones.
- Identificar mejoras en la operación y participar en la implementación de estas.

2.6. GESTION DE REDES

El proveedor deberá gestionar y administrar el Directorio Activo y sus componentes, la Red LAN, WLAN que posee el MVCT y todos los dispositivos de RED descritos en la línea base, también deberá administrar la solución de PBX Cloud con integración a office365. Descrita en el Anexo de comunicaciones Unificadas.

El proveedor deberá garantizar en la administración de los dispositivos de la red LAN y la red de Datacenter de acuerdo con lo establecido en la línea base Anexo No. 1, el poder configurar la característica de Port Mirror según lo requiera la entidad para obtener la copia del tráfico que se requiera para analizarlo en otras soluciones o dispositivos contemplados por la entidad.

El proveedor deberá gestionar la activación y desactivación de los usuarios de la Red y los servicios de office365, cumpliendo con los procedimientos establecidos en el Sistema de Gestión de Calidad del MVCT.

Se deben llevar a cabo todas las actividades de administración contempladas para este tipo de dispositivos y soluciones, así como, los análisis de cobertura y ajustes de la Red Wifi de todas las sedes del Ministerio de Vivienda, garantizando la calidad y continuidad de los servicios.

2.7. SERVICIO DE OPERACIONES DE SEGURIDAD DE LA INFORMACION (SOC)

Para soportar las necesidades que demanda el MVCT en materia de seguridad informática, se requiere que esta esté gestionada desde un punto central, que se encargue de monitorizar los eventos que ocurran tanto con los equipos de seguridad, como con el resto de la plataforma de TI. Este punto es el SOC (Security Operation Center).

En consecuencia, el MVCT, necesita tener el servicio de monitorización de su infraestructura tecnológica tanto en lo referente a seguridad informática, como a la salud y disponibilidad, durante 24 horas del día, 7 días a la semana, con unos tiempos de atención establecidos por ANS, dependiendo de la criticidad del riesgo encontrado, de manera que se puedan identificar de forma temprana las posibles amenazas que puedan comprometer la información de la Entidad, con las siguientes funcionalidades:

- Detección en tiempo real de amenazas y actividades anómalas.
- Correlación de los eventos presentados en la plataforma tecnológica desde el punto de vista de seguridad.
- Inteligencia a través de predicciones de posibles amenazas que se puedan presentar.
- Auditoría a las políticas de red y de servidores.
- Gestión adecuada y oportuna de los registros automáticos de la plataforma (Logs).
- Análisis de la ciberseguridad orientado al riesgo.
- Contribuye al cumplimiento de la norma ISO 27001 al permitir el seguimiento de los controles establecidos.
- Previene y detecta vulnerabilidades de la plataforma tecnológica e intrusiones hacia esta.
- Complementa la gestión de las herramientas de seguridad que están operativas en la Entidad.
- Protege la imagen institucional contra daños reputacionales.

2.7.1. GENERALIDADES

Durante la etapa de operación del Contrato, se deberá realizar un diagnóstico, revisar la configuración actual de seguridad, recomendar ajustes y apoyar la depuración sobre los dispositivos de seguridad anexo 1 Línea Base que actualmente tiene la entidad, anexando un reporte de hallazgos realizados, con el objetivo de identificar, analizar y optimizar el uso de políticas sin utilizar y detectar políticas duplicadas y contenidas.

El proveedor debe integrar a los servicios de mesa de ayuda el SOC para la apertura de tickets

El proveedor debe implementar, administrar, operar, soportar y actualizar la plataforma para el Monitoreo y realizar la correlación de eventos de seguridad. El proveedor debe ser partner o contar con una membresía en el más alto nivel de las soluciones ofertadas.

El SOC debe prevenir y enfrentar las diferentes situaciones de riesgos de seguridad de la información y ciberseguridad, al contar con un monitoreo proactivo, que garantice la debida gestión y optimización de las configuraciones de las tecnologías con las que cuente el Minvivienda, en los componentes del alcance del proyecto

El proveedor a través del SOC debe contar con capacidades de Inteligencia de Ciberamenazas mediante fuentes de inteligencia de indicadores de compromiso y fuentes de datos externas y de código abierto que se integran fácilmente en su plataforma de correlación. Por tanto, el oferente deberá incluir en su oferta el licenciamiento requerido para brindar en conjunto con la correlación, el servicio de Indicadores de Compromiso con el que cuente la plataforma ofertada.

Para garantizar crecimiento y adaptabilidad a los requerimientos de la entidad, se requiere que la plataforma de correlación de eventos que soporta el SOC cuente con la capacidad de monitoreo de integridad de archivos o la funcionalidad de tipo "File Integrity Monitoring" o FIM, con el fin de que se pueda monitorear los archivos críticos de información, asegurando la integridad de estos.

El proveedor deberá garantizar la configuración de como mínimo diez (10) casos de uso actuales, revisados y ajustados en conjunto con la Entidad para la puesta en operación del SOC.

2.7.2. CONDICIONES DEL SERVICIO

El proveedor debe monitorear proactivamente 7 x 24 las Plataformas y Eventos de seguridad de los componentes definidos entre el proveedor y minvivienda de la línea base establecida para una detección oportuna de amenazas y vulnerabilidades que puedan atentar contra su seguridad.

El SOC debe estar siempre disponible 7 x 24 y el proveedor debe contar con una arquitectura en alta disponibilidad que asegure una inmediata recuperación ante la falla de uno de sus componentes

El monitoreo debe incluir la evaluación del desempeño (performance), disponibilidad, transacciones sintéticas (transacciones que permiten generar carga sobre los aplicativos), uso de interfaces y estatus de procesamiento de los equipos.

El proveedor debe integrar en línea dentro del Tablero de Gestión las vistas independientes relacionadas al monitoreo de las plataformas (Eventos, Incidentes, Capacidad, etc.).

El proveedor debe realizar correlación avanzada de eventos de seguridad y ciberseguridad para proteger las plataformas de TI

El proveedor debe comunicar a Minvivienda de manera inmediata las alertas importantes de eventos, producto del monitoreo realizado, indicando las recomendaciones a seguir.

La solución base del monitoreo y alertamiento, debe soportar:

- 750 eventos por segundo (EPS)
- Mínimo 75 dispositivos a monitorear.
- Monitoreo de integridad de archivos para 25 servidores.

El SOC, deberá contar con las siguientes características:

- Actualización constante de la base de datos de contextos, configuraciones, software instalado y servidores corriendo en los dispositivos monitoreados.
- Análisis constante del desempeño de las aplicaciones lo cual permite definir atención prioritaria a la que más esté afectada mediante transacciones sintéticas.
- Visor personalizado de log de tráfico.
- Herramienta de búsqueda sobre los logs de tráfico

2.7.2.1. Características de Análisis de Seguridad en Tiempo Real.

El SOC debe contar con capacidades de analítica de eventos de seguridad y con:

- Correlación de eventos de múltiples fuentes, tales como Firewalls, Servidores, estaciones de trabajo entre otros.
- Integración por medio de APIs con fuentes de información externa sobre amenazas.
- Capacidad de hacer monitoreo de la integridad de Archivos o FIM basada en agente Windows y/o Linux.
- Capacidad de coleccionar logs de forma segura, desde dispositivos remotos.
- Tener un Framework de referencia para notificación de incidentes basado en políticas.
- Capacidad de ejecutar scripts de remediación cuando un incidente ocurra.
- Capacidad de detectar anomalías en la línea base definida.
- Detección de incidentes deberá ser en tiempo real, con capacidad de priorización para los servicios críticos.

2.7.3. SERVICIO DE OPERACIONES DE SEGURIDAD PERIMETRAL

Consiste en la prestación del servicio de administración, operación, mantenimiento renovación de los componentes de seguridad informática del MVCT incluidos en la línea base y que deben ser integrados en la operación del SOC.

El proveedor deberá incluir en el servicio al menos una capa de firewall en alta disponibilidad en cada una de las ubicaciones de los servicios de nube.

Se deben llevar a cabo todas las actividades referenciadas en el capítulo "Gestión de Servicios Aplicaciones y Bases de datos" y que apliquen en este servicio y las actividades particulares identificadas por el proveedor para estos componentes incluyendo:

1. Revisión de auditoría.
2. Eliminación, modificación y creación de reglas.
3. Eliminación, modificación y creación de componentes propios de cada componente (NATs, PATs, VPNs, túneles, configuraciones de red, reglas, etc.).
4. Liberación de mensajes en cuarentena.
5. Identificación de riesgos de seguridad y de ciberseguridad.
6. Identificación de intentos de acceso no permitido y comportamientos digitales sospechosos.
7. El proveedor deberá informar al supervisor y al oficial de seguridad cualquier incidente que se presente en las diferentes plataformas.

De igual forma se deben llevar a cabo las actividades de administración y soporte para la solución de EDR/XDR dispuesta por el MVCT para 1400 clientes que pueden crecer en un 20% y demás componentes de la solución incluyendo DLP (Data Lost Prevention) y/o cifrado de discos.

2.7.4. ACTIVIDADES ESPECÍFICAS DEL SOC

- La operación de los servicios TIC que debe soportar el proveedor deben tener calidad, trazabilidad, seguridad, escalabilidad, flexibilidad, portabilidad, reusabilidad, extensibilidad, usabilidad y mantenibilidad.
- Se requiere que el proveedor haga entrega de los procedimientos de seguridad de acceso al Datacenter.
- Garantizar la aplicación de plantillas de seguridad y prácticas de aseguramiento definidas en conjunto.
- Identificar, notificar y proponer planes de mitigación a posibles riesgos de seguridad en la operación, cambios de datos o pasos a producción (Utilización de usuarios privilegiados, usuarios o direcciones IP quemados en el código, implementación de prácticas no recomendadas en los aplicativos, puntos únicos de fallas, entre otros).
- El proveedor deberá cumplir con todas las políticas y lineamientos de la Entidad incluyendo la de seguridad y privacidad de la información definidos en el manual de políticas de seguridad y privacidad de la información y seguridad digital del ministerio de vivienda, ciudad y territorio (Anexo). así como las Directivas Presidenciales, Decretos e instrucciones que imparta Presidencia de la República, MinTIC y CSIRT.
- Actualizar con colaboración del MVCT, la matriz de activos de información con los que cuenta la entidad.

- Administrar la gestión de los riesgos digitales y de ciberseguridad de acuerdo con la metodología establecida en la norma ISO 31000 / ISO 27005 o la que el proveedor maneje que cumplan con los lineamientos dados por el Gobierno Nacional.
- Mantener las plataformas de gestión de identidades y de usuarios privilegiados de la entidad

2.8. *GESTIÓN DE INCIDENTES*

El proveedor debe participar y ser responsable en la resolución de incidentes de operación y de seguridad de la información a través de su grupo de trabajo.

El NOC y SOC deberá alertar, atender, clasificar activamente la resolución y contención de los incidentes de operación y de ciberseguridad.

El proveedor debe proporcionar recursos en la gestión y respuesta en caso de incidentes de seguridad de la información, incluyendo la detección y análisis, contención, erradicación, recuperación y actividades post-Incidentes. Estos recursos serán responsables del monitoreo y creación del ticket para el rastreo del incidente y su escalamiento a la Dirección de Tecnología de la Información y las Comunicaciones para la coordinación en su remediación

2.9. *MONITOREO DE LA SOLUCION OFERTADA*

Para garantizar la disponibilidad y seguridad de la información se requiere que el proveedor entregue dentro de su solución un servicio de gestión, monitoreo, respuesta y seguridad de la infraestructura TI del MVCT de primer y segundo nivel sobre cualquier tipo de incidente que se presente en las plataformas de servicios en tiempo real por medio de herramientas automatizadas propias del PROVEEDOR que envíen notificaciones a la Mesa de servicio de acuerdo a su nivel de criticidad y cuya información permita generar acciones proactivas, así mismo deberá Garantizar la gestión y el monitoreo de la Infraestructura en todos los servicios de nube publica y/o nube privada, desde el primer día de la operación.

El Proveedor de servicios entregará al menos una interfaz web con acceso para 5 usuarios de la herramienta de monitoreo para que el MVCT pueda revisar en tiempo real el desempeño de los servicios contratados, igualmente el monitoreo contratado debe enviar alarmas o avisos al MVCT de acuerdo con lo definido entre el MVCT y el proveedor de servicios. La interfaz de monitoreo debe proveer al menos las siguientes vistas:

1. Estado de los canales de comunicación con alertas visuales que permitan identificar condiciones de saturación o pico de tráfico excesivo (cerca al umbral o sobrepasando el umbral de uso).
2. Alertas críticas, aviso y notificación (rojas, amarillas y verde)
3. Alerta de caída o suspensión de un servicio, páginas web, aplicaciones servicios
4. Vista de mapa de servicio (vista general de infraestructura, virtualización, comunicaciones, storage y páginas web)

El proveedor debe contar herramientas especializadas de monitoreo de bases de datos, que permitan generar reportes en tiempo real de: Utilización del CPU, Utilización de la memoria, Estadísticas de conexión, Detalles del caché del búfer, Rendimiento de las consultas, Pools de recursos, Sesiones de usuarios, Detalles del interbloqueo, Errores del sistema y del usuario.

El monitoreo debe cubrir Monitoreo de Infraestructura de toda la solución, servidores (memoria, CPU y disco), almacenamiento (espacio, acceso, estado de salud, etc.), redes LAN, SAN, WiFi, seguridad, etc.

El monitoreo debe cubrir monitoreo a nivel de componentes de software, bases de datos, middleware, servidores web, etc.

El monitoreo debe generar alertas por errores y condiciones críticas en los logs y los elementos de la solución que permitan identificar fallas de manera proactiva.

El monitoreo también deberá reportar de manera semanal:

- Vistas actualizadas de infraestructura.
- Reportes de ocupación y proyecciones de recursos
- Reportes de Backup
- Reportes de fallo y escalamientos

No obstante, lo anterior, el Proveedor está en la obligación de informar y notificar al Equipo de Supervisión, cualquier incidente y novedad que afecte los sistemas de información y aplicaciones generados en la herramienta de gestión.

2.10. REPORTES

El proveedor deberá entregar reportes predefinidos y deberá permitir crear reportes personalizados. Reportes mínimos priorizados por los activos críticos:

- Informe mensual de las actividades realizadas del monitoreo y alertamiento.
- Informe quincenal de incidentes de seguridad que hayan sido detectados
- Informe mensual de disponibilidad.
- Informe mensual de Rendimiento.

Otros reportes acordes con el monitoreo y de común acuerdo con el supervisor del contrato podrán ser:

- Ataques de denegación de servicios (DDoS).
- Incidentes de seguridad.
- Actividades Sospechosas de Usuarios / Equipos / Aplicaciones.
- Integridad de Archivos.
- Cambios de Configuraciones.
- Cambios no Autorizados en los Registros de Windows.
- Violaciones de Políticas de Control de Acceso.
- Disponibilidad.

- Rendimiento o Recursos.
- Caídas en Servicios y en Aplicaciones.
- Cambios en los Registros.
- Cambios en el Software Instalado.
- Cumplimiento de acuerdos de nivel de servicio
- Abusos de Privilegios de Navegación.
- Malware en el mes.
- Ataques a la infraestructura.
- Usuarios con Malware
- Usuarios con Botnets.
- Aplicaciones maliciosas en la Red.
- Exploits Detectados.
- Usuarios/ Equipos más Riesgoso para la entidad.
- Categorías más usadas por los usuarios.
- Destinos maliciosos de la red.
- Usos de la VPN a horas no laborales.
- Segmentos de Red comprometidos

2.11. *TABLEROS DE GESTIÓN*

La gestión del NOC y SOC se debe reportar mediante un tablero de Gestión visible para la Entidad, que proporcione un resumen ejecutivo y un cuadro de mandos, con el estado en tiempo real (incluyendo los cumplimientos de los ANS comprometidos), así como, con la información detallada, sus responsables y presentación gráfica de la funcionalidad monitoreada en tiempo real.

En el tablero se podrá realizar un seguimiento a través de acuerdos de nivel de servicio (ANS) e indicadores clave de desempeño en ingles Key Performance Indicator (KPI's) continuamente actualizados.

El tablero debe permitir realizar configuraciones de vistas resumidas que puedan ser personalizables y que contengan la información técnica de las plataformas que se encuentran bajo gestión.

El tablero debe contar con vistas de acuerdo con los roles necesarios para los diferentes niveles que indique el Ministerio de Vivienda Ciudad y Territorio.

El tablero del NOC y SOC debe contar con una disponibilidad superior al 99.5%.

2.12. *DRP*

Las aplicaciones iniciales definidas por MVCT sobre las cuales se ejecutará el servicio DRP son:

- Sistema de Inversiones en Agua Potable y Saneamiento Básico - SINAS

- Sistema de Gestión de Información de Viceministerio de Agua y Saneamiento Básico - SIGEVAS
- Gestión Documental - GESDOC
- Sistema de subsidio familiar de vivienda – SISFV

2.12.1. GENERALIDADES

El servicio de DRP, deberá contar con los equipos activos de red requeridos para la conectividad y correcto funcionamiento del servicio.

Deberá contar con la capacidad computacional y la capa de almacenamiento necesario para el funcionamiento de las aplicaciones en contingencia, sobre la cual operará los servicios de DRP.

Durante la ejecución del contrato, el MVCT y el proveedor de común acuerdo y según la metodología de control de cambios, podrán desmontar aplicaciones, definir e implementar nuevas, en caso de no lograrse un acuerdo, prevalecerán los definidos en el contrato.

Durante la etapa de definición e implementación del servicio, los especialistas por parte del proveedor definirán y presentarán al MVCT los planes y actividades a desarrollar a fin de cumplir con el objetivo del servicio de DRP, la cual se debe realizar dentro de los primeros cuatro meses siguientes a la entrada en operación del servicio de Datacenter Principal. Igualmente, los especialistas por parte del proveedor deberán integrarse para las actividades que se deriven de los controles de cambios implementados, así como, durante la declaración de la contingencia.

El proveedor debe cumplir de conformidad con lo exigido, con el plan de montaje de la solución del servicio del DRP, incluyendo cronograma y plan de trabajo, recursos físicos, humanos y responsables para cada actividad y fase del plan, que deberá llevarse a cabo durante la ejecución del contrato y estar en concordancia con las actividades planeadas en el sitio principal.

El proveedor deberá revisar el “Anexo 1: Línea base.xlsx” a fin de verificar la correlación de servicios e infraestructura a fin de garantizar la prestación de servicio DRP.

2.12.2. CONDICIONES DEL SERVICIO

Punto objetivo de recuperación (RPO): Se fija como tiempo anterior de punto de recuperación máximo de 40 minutos

El punto objetivo de recuperación es conceptualmente el tiempo que transcurre entre el registro de una transacción en el centro de datos principal y el registro de esta en la solución definida para el servicio de DRP.

El Proveedor deberá suministrar una solución de replicación real de datos, sin afectar el desempeño actual de las aplicaciones y que garantice el cumplimiento de los niveles de servicio (RTO, RPO), solicitados en el presente Anexo.

La solución de replicación deberá operar con la misma eficiencia y confiabilidad independientemente de la distancia entre el centro de datos principal y la solución definida para el servicio de DRP.

El monitoreo de la solución definida para el servicio de DRP se deberá integrar a la solución de monitoreo propuesta para el sitio principal, así mismo, se debe suministrar un acceso a la interfaz web de la herramienta de gestión para que el Ministerio pueda visualizar el estado de los componentes del DRP.

Tiempo Objetivo de Recuperación (RTO): El Tiempo de Recuperación Objetivo RTO será de máximo 4 horas.

El Proveedor deberá elaborar, implementar, ejecutar y actualizar los procedimientos para la activación de los servicios tecnológicos cuando se declare la contingencia.

El Proveedor debe actualizar el procedimiento para volver a la normalidad una vez haya pasado la contingencia.

El Proveedor durante la ejecución de las pruebas deberá afinar los procedimientos y mecanismos utilizados en las mismas.

El Proveedor se compromete a documentar cada una de las pruebas realizadas e incluirlas en la documentación del proyecto. El Proveedor debe actualizar los procedimientos asociados al plan de pruebas y simulacros del servicio de DRP.

Se deberán realizar en el año como mínimo dos (2) pruebas de contingencia sobre las cuatro (4) aplicaciones definidas.

2.12.3. REQUISITOS ESPECIFICOS DE LA SOLUCION

1. Realizar la implementación de la arquitectura de seguridad interna que proteja de accesos no autorizados y que brinde seguridad a la información contenida en los servidores, los cuales deberán ser ubicados en segmentos de red protegidos por firewalls internos.
2. Incluir todos los equipos de seguridad y el software correspondiente requeridos para el correcto funcionamiento y protección de la información relacionada con las aplicaciones definidas para el servicio DRP.
3. Incluir los equipos de almacenamiento necesarios para soportar las necesidades de procesamiento alternativo con soporte de sistemas operativos, bases de datos, aplicaciones y demás configuraciones pertinentes.

4. Incluir licenciamiento tanto para sistemas operativos, plataforma de virtualización, sistemas de almacenamiento, plataforma de replicación, plataforma de backups y respaldo, software requerido a nivel de aplicación, base de datos demás que tenga que ver con los servicios para la implementación requerida por el MVCT.
5. Se debe garantizar la replicación de la información de las aplicaciones implementadas en el servicio de DRP, de manera que se pueda dar cumplimiento en el 100% de los acuerdos de nivel de servicio del sitio principal.
6. Apoyo en la administración de sistemas operativos una vez en contingencia.
7. El servicio de replicación de información debe garantizar que las aplicaciones y servicios del Centro de Datos Principal seleccionadas para la contingencia, tengan una copia de sus datos en el servicio definido para la recuperación en caso de desastre.
8. Se debe suministrar el servicio de monitoreo y control del desempeño de los servicios y optimización de los recursos disponibles de la solución definida.
9. El proveedor debe efectuar la elaboración, implementación, ejecución y actualización de los procedimientos de administración y operación del servicio sitio principal, en cuanto a manuales y configuraciones existentes para poder atender óptimamente los requerimientos de DRP y continuidad de los sistemas, equipos TIC y servicios solicitados y en cumplimiento de los niveles de servicio requeridos para el MVCT.
10. El proveedor debe actualizar, definir y documentar los roles y responsabilidades de tipo administrativo y operativo que se deberán tener en cuenta en el momento en que el servicio quede en producción.
11. El proveedor debe ofrecer todos los mecanismos, herramientas y procedimientos necesarios para mantener los niveles de disponibilidad requeridos y exigidos por el MVCT.
12. El proveedor debe realizar y actualizar los procedimientos de backups y restauración de información entre los Centros de Datos Principal y la infraestructura definida para el cumplimiento de los objetivos del servicio de DRP.
13. Para los cambios requeridos sobre la plataforma y servicios contratados el Proveedor se debe acoger al proceso de administración del cambio, con el objeto de poder dar cabal cumplimiento de los acuerdos de niveles de servicios definidos en el presente pliego de condiciones.
14. El proveedor debe presentar mensualmente informes de la gestión realizada entre los Centros de Datos (principal y la solución definida para el servicio de DRP).
15. El proveedor deberá brindar soporte de operación 7X24x365, a los requerimientos de DRP y continuidad del negocio acordado con el MVCT entre el centro de datos principal y servicio de DRP.

16. Al finalizar el contrato, el proveedor debe entregar a la oficina TIC, toda la documentación, manuales y procedimientos actualizados relacionados con la operación del sitio principal y la solución definida para la gestión de DRP.
17. El Servicio de DRP deberá cumplir con las normas de distancia mínima de 15Km entre Datacenter Principal y al Datacenter alternativo y contingencia que permitan entrar en operación ante fallas de disponibilidad de las aplicaciones definidas.
18. Realizar los mantenimientos técnicos preventivos (mínimo una vez al año) y correctivos de los equipos suministrados para la ejecución del contrato, llevar una hoja de vida y bitácora respectiva para cada uno de los elementos de la infraestructura como parte de la documentación inherente a la ejecución del proyecto, las cuales deberán ser entregadas como parte del informe mensual de gestión. El Proveedor deberá entregar a los supervisores del contrato el plan de mantenimiento preventivo una vez implementados los servicios.
19. El proveedor debe ofrecer una solución de replicación real de datos, sin afectar el desempeño actual de las aplicaciones y que garantice el cumplimiento de los niveles de servicio (RTO, RPO) solicitados por el MVCT.
20. El proveedor debe garantizar que la solución de replicación operará con la misma eficiencia y confiabilidad independientemente de la distancia entre el sitio alternativo y principal
21. El proveedor debe suministrar el servicio de administración, operación y soporte de toda la infraestructura disponible para el normal funcionamiento de la solución definida para el DRP.
22. El proveedor debe suministrar el servicio de monitoreo y control del desempeño de los servicios y optimización de los recursos disponibles en la solución definida para el DRP.
23. Gestionar (operar y administrar) la plataforma tecnológica de la solución definida para el DRP, durante el tiempo que dure la recuperación de los servicios de tecnología en los Centros de Datos Principal o mientras el MVCT lo determine. Además, deberá realizar en conjunto con el MVCT los procedimientos de retorno a la normalidad de las operaciones del Centro de Datos Principal.
24. El proveedor deberá elaborar, implementar, ejecutar y actualizar los procedimientos para la activación de los servicios tecnológicos cuando se declare la contingencia.
25. El proveedor debe actualizar sí se requiere el procedimiento para activar el plan de contingencia.
26. El proveedor debe actualizar el procedimiento para volver a la normalidad una vez haya pasado la contingencia.
27. Se deberán realizar en el año como mínimo dos (2) pruebas de contingencia sobre las cuatro (4) aplicaciones definidas. El objetivo de estas pruebas es verificar la

funcionalidad y configuración de los equipos y servicios ofrecidos por el proveedor del mismo modo, se podrá verificar y corroborar la funcionalidad de los procedimientos internos del MVCT en el momento de una contingencia.

28. El proveedor, durante la ejecución de las pruebas deberá afinar los procedimientos y mecanismos utilizados en las mismas.
29. El proveedor se compromete a documentar cada una de las pruebas realizadas y a incluirlas dentro de la documentación del proyecto.
30. Ante la presencia de interrupciones o desastres mayores de alto impacto que impidan el normal funcionamiento del sitio principal, la solución definida para el DRP debe suministrar los servicios y acceso a las aplicaciones que en el estén implementadas con los niveles de servicio solicitados.
31. El proveedor debe actualizar los procedimientos asociados al plan de pruebas y simulacros de la solución definida para el servicio de DRP.
32. Los servicios se podrán levantar de manera individual o levantar toda la solución implementada. Para ambos casos deben quedar documentados y probados los diferentes procedimientos.
33. El proveedor debe ofrecer todos los mecanismos, herramientas y procedimientos necesarios para llevar a cabo el plan de contingencia acorde al RPO y RTO.

Servicios de Conectividad

Se debe proveer un (1) enlace dedicado para comunicar la sede administrativa (centro de datos principal), con la solución definida del servicio de DRP, con un ancho de banda de 100 Mbps.

Se debe proveer un (1) acceso desde solución definida del servicio de DRP, hacia Internet con ancho de banda efectivo de 60 Mbps para anunciar públicamente los servicios requeridos hacia internet (1:1) sin reuso y disponibilidad de 99,99%, ambos canales deberán tener capacidad de crecimiento futuro.

En el evento de presentarse una situación de no operación o desastre en el centro de datos principal, todas las comunicaciones WAN deben ser, redireccionadas a la solución definida del servicio de DRP en un tiempo no mayor a 30 Minutos.

Se debe realizar toda la gestión necesaria para publicar los hosts en internet, así como el suministro de direccionamiento público requerido.

Se deben incluir DNS alternos, que permitan garantizar alta disponibilidad en la resolución de nombres de los servidores publicados.

seguridad informática

El Proveedor deberá realizar la implementación de la arquitectura de seguridad interna que proteja de accesos no autorizados y que brinde seguridad a la información contenida en los servidores, los cuales deberán ser ubicados en segmentos de red protegidos por firewalls internos.

El proveedor debe suministrar los mecanismos mínimos necesarios para proteger de ataques informáticos las conexiones que se hagan entre el Centro Principal y la solución definida del servicio de DRP, asignando los segmentos de red protegidos que correspondan, VPNs, y zonas desmilitarizadas entre otras, mientras este tráfico deba ser publicado o pase por internet.

Los servidores deberán estar protegidos mediante VLANs separadas por firewall dedicadas exclusivamente al MVCT.

Para la publicación en Internet el proveedor deberá suministrar protección mediante sistema de prevención de intrusos (IPS), inundación de tráfico, denegación del servicio (DoS, DDoS), entre otros.

Acuerdos de Niveles de Servicio

Los ANS serán los mismos establecidos para las aplicaciones iniciales definidas por MVCT para el servicio de Datancenter (principal) sobre las cuales se ejecutará el servicio DRP y serán aplicables desde el momento en que se cumplan el RPO y RTO.

Las aplicaciones son:

- Sistema de Inversiones en Agua Potable y Saneamiento Básico - SINAS
- Sistema de Gestión de Información de Viceministerio de Agua y Saneamiento Básico - SIGEVAS
- Gestión Documental - GESDOC
- Sistema de subsidio familiar de vivienda - SISFV

3. OTROS SERVICIOS

3.1. CUSTODIA DE MEDIOS

Proveer y mantener vigente durante la duración del servicio la custodia de medios que cuenten con: almacenamiento, transporte de medios magnéticos, bóvedas especiales, personal capacitado en la manipulación de información y estrictas medidas de seguridad, que permitan garantizar la conservación y seguridad de la información, el servicio se debe proveer para un total de 900 medios de los cuales hay 678 LTO6, las demás LTO3.

4. DOCUMENTOS RELACIONADOS

A fin de implementar el proyecto, EL PROVEEDOR debe contemplar con carácter obligatorio los requerimientos establecidos por parte del MVCT en este documento y debe garantizar el suministro de los elementos de Hardware, Software, activos y recursos que sean detallados en el mismo y/o los que sean necesarios para el desarrollo de sus actividades y debe garantizar los servicios con la calidad ofertada, la cual no puede ser inferior a la solicitada en los siguientes Anexos:

- Anexo 1 - Líneas base
- Anexo 2 - Acuerdos Niveles de Servicio
- Anexo 8 - políticas de backup