Proyecto

“Actualización tecnológica para el fortalecimiento de las finanzas públicas”

2023-2024

Quito, Octubre de 2022

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

1. DATOS INICIALES DEL PROYECTO

1.1 Tipo de Solicitud de Dictamen

Dictamen de prioridad (Proyecto Nuevo)

1.2 Nombre Proyecto

Actualización tecnológica para el fortalecimiento de las finanzas públicas (CUP 81300000.0000.388355)

1.3 Entidad (UDAF)

Ministerio de Economía y Finanzas del Ecuador

1.4 Entidad Operativa Desconcentrada (EOD)

La Institución que se encargará de la ejecución del proyecto es el Ministerio de Economía y Finanzas del Ecuador a través de la Subsecretaría de Innovación de las Finanzas Públicas

1.5 Gabinete Sectorial

Gabinete Sectorial Económico

1.6 Sector, subsector y tipo de inversión

De acuerdo con la matriz de clasificación de macrosector sectores y subsectores, el proyecto se enmarca en:

Tabla 1 Macro Sector, Sector y Subsector

Macro Sector	Sector		Subsector
MULTISECTORIAL	Manejo Fiscal	D1901	Administración Fiscal

T02 Equipamiento: El tipo de inversión del proyecto involucra la adquisición de equipamiento para el sostenimiento del sistema de administración financiera que permita brindar un mejor servicio a las entidades del Estado usuarias del sistema e-SIGEF.

1.7 Plazo de ejecución

El proyecto inicia el 01 de enero de 2023 y finaliza el 29 de febrero de 2024.

1.8 Monto total

El monto total del proyecto es de USD 6.684.139,84 (Seis millones seiscientos ochenta y cuatro mil ciento treinta y nueve dólares de los Estados Unidos de Norteamérica con ochenta y cuatro centavos).

De este monto, USD 6.684.139,84 corresponde al aporte del Banco Interamericano de Desarrollo – BID. Estos fondos provienen del crédito 4812 OC-EC.

Tabla 2 Monto Total requerido por el proyecto anualmente

Año	2023	2024	TOTAL
Monto Dólares	5.162.171,02	1.521.968,82	6.684.139,84

Fuente: Subsecretaría de Innovación de las Finanzas Públicas
Elaboración: Equipo del proyecto

2. DIAGNÓSTICO Y PROBLEMA

2.1 Descripción de la situación actual del sector de intervención y de influencia por el desarrollo del proyecto

El Ministerio de Economía y Finanzas como Ente Rector de las Finanzas Públicas brinda a las instituciones del sector público, el servicio de las aplicaciones tecnológicas: eSIGEF, SPRYN, eSByE, Interoperabilidades, además de administrar el Sistema de Gestión y Análisis de Deuda SIGADE, entre las principales.

El sistema e-SIGEF dispone actualmente de los módulos de Presupuesto, Contabilidad y Tesorería, siendo su enfoque operativo totalmente presupuestario. La capacidad transaccional con la herramienta medida en número de usuarios es de aproximadamente 11.290 usuarios.

El sistema SPRYN, que tiene un número de usuarios que lo operan de: 3765 es el responsable de la generación de los procesos de remuneraciones y nómina de todo el sector público, llegando a generar aproximadamente 4000 o 5000 nóminas al mes con 500.000 de funcionarios públicos por mes.

El sistema eSByE, que tiene un número de usuarios que lo operan de: 3621, es el responsable de la gestión de los bienes y las existencias de las entidades del sector público que pertenecen al Presupuesto General del Estado, incluyendo un módulo de inventarios, gestionando actualmente se tiene 10´186.189 bienes aprobados y contabilizados, de 1091 instituciones.

Los sistemas de las finanzas públicas interoperan con las siguientes entidades: Banco Central, Servicio de Rentas Internas, Instituto Ecuatoriano de Seguridad Social, Servicio Nacional de Contratación Pública, Dirección Nacional de Registros Públicos, Corporación Nacional de Telecomunicaciones, entre los más importantes. Intercambiando información con 48 puntos de interconexión.

El SIGADE es el Sistema de gestión y análisis de deuda, construido por la UNCTAD (Conferencia de las Naciones Unidades sobre Comercio y Desarrollo) diseñado para la gestión, control y administración de la deuda del Ecuador, proporcionando información exacta y oportuna, como un elemento de análisis, estrategia y sostenibilidad. Tiene un número de usuarios de: 12.

2.1.1 Infraestructura del Sistema de las Finanzas Públicas

Para mantener su disponibilidad y continuidad de los servicios de las aplicaciones antes indicadas, esta Cartera de Estado ha realizado inversiones en su infraestructura y plataforma tecnológica a lo largo de los años, para cubrir y solventar las diferentes necesidades tecnológicas.

La infraestructura tecnológica que da soporte a los sistemas de las finanzas públicas, está conformada por equipos servidores utilizados en el funcionamiento de las diferentes capas que integran la solución, equipos cuyas características se describe a continuación:

Tabla 3 Equipos Servidores

Capa / Utilidad	*Cantidad*	*Hardware*	*Software*	*Observaciones*
Nube Privada	**16**	4 procesadores Intel ® Xeon ® CPU E5-4640 2.40 GH 256 GB RAM 2 tarjetas de RED HP Flex-10 10Gb 2-port 530FLB Adapter 2 tarjetas de fibra QLogic QMH2572 8Gb FC HBA for HP BladeSystem c-Class 2 discos internos de 300 GB SAS	Windows 2012 Server x64 Standard Edition.	
Presentación	**2**	12 Virtual Cores Intel ® Xeon ® CPU E5-4640 2.40 GHz 12 GB RAM	Windows 2003 Server R2 x64 Standard Edition SP2.	Servidores Virtuales
	2		Windows 2012 Server x64 Standard Edition.	
Aplicación	**2**	12 Virtual Cores Intel ® Xeon ® CPU E5-4640 2.40 GHz 12 GB RAM	Windows 2003 Server R2 x64 Standard Edition SP2.	Servidores Virtuales
	19		Windows 2012 Server x64 Standard Edition.	
Reportes	**3**	12 Virtual Cores Intel ® Xeon ® CPU E5-4640 2.40 GHz 12 GB RAM	Windows 2012 Server x64 Standard Edition.	Servidores Virtuales
Biometría App	**1**	Un (1) Procesador Intel® Xeon® Processor X5560 (2.80 GHz, 8MB L3 Cache, 95W, DDR3-1333, HT, Turbo 2/2/3/3) Dos (2) puertos SAN FiberChannel de	Windows Server 2008 R2 x64	No tiene discos

Capa / Utilidad	*Cantidad*	*Hardware*	*Software*	*Observaciones*
		8Gbps 8 GB RAM	Standard Edition SP1.	internos físicos
Biometría BDD	**1**	Un (1) Procesador Intel® Xeon® Processor X5560 (2.80 GHz, 8MB L3 Cache, 95W, DDR3-1333, HT, Turbo 2/2/3/3) Dos (2) puertos SAN FiberChannel de 8Gbps 8 GB RAM	Windows Server 2008 R2 x64 Standard Edition SP1.	No tiene discos internos físicos
Base de Datos	**2**	HP Integrity SuperDome2 3 celdas 256 GB RAM Intel(R) Itanium(R) Processor 9560 (2.53 GHz, 32 MB) 48 logical processors 4 Tarjetas de Red PCI-E de 10Gbps Ethernet 4 Tarjetas de Fibra PCI-E de 16Gbps FC Qlogic	SO HP-UX 11i V3 Oracle Enterprise 11.2.0.3.0	Rack Producción
GRID Control de Oracle	**1**	Dos (2) Procesador Intel® Xeon® Processor X5560 (2.80 GHz, 8MB L3 Cache, 95W, DDR3-1333, HT, Turbo 2/2/3/3) Dos (2) puertos SAN FiberChannel de 8Gbps Cuatro (4) puertos LAN de 10Gbps Ethernet	Sistema Operativo Linux Red Hat EL 5.2 x64	
Base de Datos BI	**1**	HP Integrity SuperDome2 140 GB RAM Intel(R) Itanium(R) Processor 9560 (2.53 GHz, 32 MB) 5 logical processors 4 Tarjetas de Red PCI-E de 10Gbps Ethernet 4 Tarjetas de Fibra PCI-E de 16Gbps FC Qlogic	SO HP-UX 11i V3 Oracle Enterprise 11.2.0.3.0	
Sistema de Almacenamiento	**1**	HPE StoreServ 3PAR 20450 (2 Nodes) Service Processor 400 GB de cache para el manejo de la información de datos y de control 24 puertos Fiber Channel a 16Gbps 2 puertos para administración. RJ45 de 1 Gbps 6 Disk Ports 24 discos de estado sólido 7.6 TBi- 170 TB Fuentes de poder redundantes internas, con la característica de instalación en caliente (hot-swap/plug). 200 a 240 VAC, 50 a 60 Hz	3.3.1.410 (MU2)	
Switches Directores	**2**	San Director SN8000B 2 módulos redundantes de procesamiento de control, hot swap/plug, independientes de los módulos de conmutación e interconexión 2 módulos para interconexión con otros Switch SAN Directors. Velocidad de conexión externa de 16Gbps Ancho de banda >= 1 Tbps, sin utilizar puertos Fiber channel de los módulos de conmutación. 48 puertos de 16 Gbps Fiber Channel, por cada equipo switch San Director. Ancho de banda >= 768 Gbps		

Capa / Utilidad	*Cantidad*	*Hardware*	*Software*	*Observaciones*
	2	SAN Director 4/256 Módulo de procesamiento redundante Velocidad de conexión externa de 8Gbps Protocolos soportados FC, FC-ip, iSCSI 64 puertos de 8Gbps 4 puertos iSCSI Fuentes de poder redundantes trabajando a 220V Instalados en rack de 42U de comunicaciones SAN		

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo gestión del proyecto

Como infraestructura de comunicaciones el Ministerio de Economía y Finanzas dispone:

Tabla 4 Equipos de Comunicaciones

Sistema /Tipo	Cantidad	Hardware
Firewall externos	2	Marca Cisco ASA5540 Esquema de StatefulFailover Activo/ Standby, Sistema IDS/IPS ASA SSM-10 interface 10/100/100 Mbps y cuatro interfaces
Firewall internos	2	Marca Cisco ASA5580-20 Esquema StatefulFailover Activo/Standby Sistema IDS/IPS ASA SSM-10 interface 10/100/1000 Mbps y seis interfaces.
SwitchCore	1	Marca Cisco 6509-E Dos (2) tarjetas supervisoras VS-S720-10G Modalidad SSO (StatefulSwitchover)
SwitchCore	1	Marca HPE 7910 >= (2) dos módulos de Entrada/Salida (I/O) - 24 puertos de 10 GbE cada uno 8 GB RAM

Fuente: Subsecretaría de Innovación de las Finanzas Públicas
Elaboración: Dirección Nacional de Operaciones

El proveedor del canal de Internet es CNT con un ancho de banda de 40 mbps actualizable, servicio última milla redundante con fibra óptica y TELCONET con ancho de banda de 40 mbps, última milla redundante con fibra óptica.

Para la obtención de respaldos se dispone de una librería física de respaldos marca HP, librería física ESL322e con las siguientes características:

Tabla 5 Equipos de Respaldos

Ítem	*Configuración*
Brazo robótico	1 brazo robótico situado en la parte interna del módulo.
Controlador de la librería física.	Localizado en la parte posterior del rack sección superior.
Módulo de administración.	Localizado en la parte posterior del rack sección inferior.
Librerías físicas	2 librerías físicas, cada librería compuesta de 4 drives.
Medios de almacenamiento (cartuchos)	250 de 1.6 TB de capacidad, modelo Ultrium LTO 4

Fuente: Subsecretaría de Innovación de las Finanzas Públicas
Elaboración: Dirección Nacional de Operaciones

Además, se dispone de un almacenamiento EVA 4000 con 84 discos FC de 450 GB cada uno que sirve como almacenamiento para la librería VLS12000. Todo el sistema de respaldos esta manejado a través del software Data Protector versión A.06.11

Solución de respaldos VLS 12000. Características:

Tabla 6 Solución de Respaldos

Item	*Configuración*
Procesador	Quad Core 2.5Ghz 1333
Discos	2 discos sata de 120GB cada uno en raid 1
Memoria	16 GB en memoria Ram
Nic	2 tarjetas de red Nic 1, para servicio private Nic 2, para servicio public
Hba	1 tarjetas hba con 4 puertos de Fibra 2 puertos para storage y 2 puertos para hosts
Fuentes de poder	2 fuentes de poder redundantes
Tamaño en Unidades de rack	1 U
Controlador del storage	2 controladores que trabajan en modo redundante.
Cajas de discos	8 cajas de discos. En total se instaló 84 discos del tipo FC de 450GB cada uno y una velocidad de 10k.

Fuente: Subsecretaría de Innovación de las Finanzas Públicas
Elaboración: Dirección Nacional de Operaciones

Junto al sistema e-SIGEF se ha implementado bajo el mismo modelo de arquitectura, el sistema SPRYN que permite obtener la información relacionada con la ejecución del presupuesto de remuneraciones y cuya infraestructura responde a las siguientes características:

Tabla 7 Infraestructura sistema SPRYN

Capa / Utilidad	*Cantidad*	*Hardware*	*Software*	*Observaciones*
Aplicación	8	12 Virtual Cores Intel ® Xeon ® CPU E5-4640 2.40 GHz 40 GB RAM	RedHat Enterprise 7	Servidores Virtuales

Fuente: Subsecretaría de Innovación de las Finanzas Públicas
Elaboración: Dirección Nacional de Operaciones

Para el almacenamiento de información comparte el sistema HP 3PAR 20400 del e-SIGEF.

Como elementos de contingencia se ha definido la siguiente configuración:

- Clúster de servidores en configuración de balanceo de carga (F5) y configuración Oracle RAC para los servidores de Base de Datos.
- Configuración en el almacenamiento de discos de estado sólido con arreglos de discos en Raid 5.
- Plantilla de seguridad en línea de base para servidores virtuales de aplicaciones y reportes.

La redundancia manejada a través de Directorio Activo esta implementado en servidores con las siguientes características:

Tabla 8 Servidor de Directorio Activo

Capa / Utilidad	*Cantidad*	*Hardware*	*Software*	*Observaciones*
Active Directory	3	4 Virtual Cores Intel ® Xeon ® CPU E5-4640 2.40 GHz 8 GB RAM	Windows 2012 R2 Server x64 Standard Edition.	Servidores Virtuales

Fuente: Subsecretaría de Innovación de las Finanzas Públicas
Elaboración: Dirección Nacional de Operaciones

Los equipos destinados a la protección de la red y comunicaciones Firewall se han configurado en forma redundante y es administrado por el fabricante mediante un contrato de mantenimiento CustomRepair.

Para los equipos que dan soporte al tema de inteligencia de negocios no se han definido mecanismos de contingencia.

Tabla 9 Infraestructura del BI-Cognos

Capa / Utilidad	Cantidad	Hardware	Software	Observaciones
BI (Cognos) Presentación Producción	1	12 Virtual Processors Intel ® Xeon ® CPU E5-4640 2.40 GHz 24 GB RAM	Windows Server 2008 R2 x64 Standard Edition.	Servidor Virtual
BI (Cognos) Aplicación Producción	1	12 Virtual Processors Intel ® Xeon ® CPU E5-4640 2.40 GHz 24 GB RAM	Windows Server 2008 R2 x64 Standard Edition.	Servidor Virtual
BI Planning Producción	1	8 Virtual Processors Intel ® Xeon ® CPU E5-4640 2.40 GHz 24 GB RAM	Windows 2012 R2 Server x64 Standard Edition.	Servidor Virtual
BI (Cognos) Presentación Desarrollo	1	1 Processors 8 cores Intel ® Xeon ® CPU X5560 2.80 GHz 12 GB RAM	Windows Server 2008 R2 x64 Standard Edition.	Servidor Físico
BI (Cognos) Aplicación Desarrollo	1	1 Processors 8 cores Intel ® Xeon ® CPU E5-4640 2.40 GHz 24 GB RAM	Windows Server 2008 R2 x64 Standard Edition.	Servidor Físico
BI Planning Desarrollo	1	6 Virtual Processors Intel ® Xeon ® CPU X5560 2.80 GHz 12 GB RAM	Windows 2012 R2 Server x64 Standard Edition.	Servidor Virtual

Fuente: Subsecretaría de Innovación de las Finanzas Públicas
Elaboración: Dirección Nacional de Operaciones

Tabla 10 Infraestructura de Base de datos del BI-Cognos

Capa / Utilidad	Cantidad	Hardware	Software	Observaciones
BDD BI Producción	1	5 logical processors (5 per socket)	HP-UX B.11.31	Servidor Virtual
		Intel(R) Itanium(R) Processor 9560 (2.53 GHz, 32 MB)		
		90 GB RAM		
BDD BI Desarrollo	1	8 virtual processors	Red Hat Enterprise Linux Server release 5.2 (Tikanga)	Servidor Físico
		Intel(R) Xeon(R) CPU X5560 @ 2.80GHz 24 GB RAM		

Fuente: Subsecretaría de Innovación de las Finanzas Públicas
Elaboración: Dirección Nacional de Operaciones

La infraestructura física del centro de cómputo está conformada por los siguientes elementos:

- Sistema de control de acceso al centro de datos mediante dispositivo biométrico.
- Sistema de acometida eléctrica exclusiva al Ministerio de Economía y Finanzas con transformador eléctrico y cámara de transformación.
- Sistema de generación eléctrica alterno mediante equipo Caterpillar de 280 KVA, en operación normal con contrato de mantenimiento preventivo y correctivo.
- 2 unidades de poder sin interrupción (UPS) General Electric de 100 KVA de alta disponibilidad con 10 horas de autonomía e instalaciones eléctricas separadas, una por cada UPS´s a fin de conectar las fuentes de los equipos una en cada UPS´s, en operación normal y bajo un contrato de soporte post garantía por un año.
- Tablero automático de transferencia entre la red normal y el equipo de generación. Estado actual: operación normal y con contrato de mantenimiento preventivo y correctivo.
- Sistema de aire acondicionado para el área de UPS y Centro de Datos. 2 unidades LG de 60 000 BTU cada una para el área de UPS's y 2 unidades Stulz de 170 000 BTU para el Centro de Datos. Las Unidades LG se encuentran bajo un contrato de mantenimiento preventivo y correctivo por un año y las unidades Stulz mediante un contrato de soporte post garantía por un año.
- Sistema de detección y extinción automática de fuego mediante 1 bombona de gas Ecaro 25 (HFC-125), panel de control y sensores iónicos y fotoeléctricos. Este sistema está con un contrato de soporte post garantía por un año.
- Sistema de monitoreo de alarmas y eventos relacionados con energía eléctrica, sistema de aire acondicionado, detección y extinción de fuego, temperatura, control de acceso físico a las áreas críticas, sensores de vibración y sensores de agua. El sistema se halla en operación normal y bajo un contrato de soporte post garantía por un año.
- Sistema de vigilancia por video cámaras basado en la red de datos (IP), monitoreo que se extiende a todo el edificio mediante 25 cámaras distribuidas en el edificio y en el centro de cómputo, software para administración del sistema.

El Ministerio de Economía y Finanzas posee además un Centro de Datos Alterno en la ciudad de Guayaquil, en el que se encuentra la réplica de la base de datos transaccional y de las aplicaciones: eSIGEF, SPRYN y eSByE. A continuación, se describe sus características:

Tabla 11 Centro de datos Alterno (capacidades y servicios)

Servicio	Cantidad	Hardware	Software	Observaciones
SPRYN aplicación	4	3 Virtual Processors por cada servidor Intel(R) Xeon(R) CPU E5-2690 0 @ 2.90GHz 20 GB RAM por cada servidor	Red Hat Enterprise Linux 8 (64-bit)	Servidor Virtual
interoperabilidad aplicación y presentación	2	4 Virtual Processors por equipo Intel(R) Xeon(R) CPU E5-2690 0 @ 2.90GHz 8 GB RAM por equipo	Microsoft Windows Server 2012 R2 (64-bit)	Servidor Virtual
eSigef aplicación	4	4 Virtual Processors por cada servidor Intel(R) Xeon(R) CPU E5-2690 0 @ 2.90GHz 8 GB RAM por cada servidor	Microsoft Windows Server 2012 R2 (64-bit)	Servidor Virtual
eSigef reportes	1	4 Virtual Processors Intel(R) Xeon(R) CPU E5-2690 0 @ 2.90GHz 8 GB RAM	Microsoft Windows Server 2012 R2 (64-bit)	Servidor Virtual
eSipren	2	4 Virtual Processors por cada servidor Intel(R) Xeon(R) CPU E5-2690 0 @ 2.90GHz 8 GB RAM por cada servidor	Microsoft Windows Server 2012 R2 (64-bit)	Servidor Virtual
eByE	1	4 Virtual Processors Intel(R) Xeon(R) CPU E5-2690 0 @ 2.90GHz 8 GB RAM	Microsoft Windows Server 2012 R2 (64-bit)	Servidor Virtual
File server eSigef	1	4 Virtual Processors Intel(R) Xeon(R) CPU E5-2690 0 @ 2.90GHz 8 GB RAM	Microsoft Windows Server 2012 R2 (64-bit)	Servidor Virtual
Active Directory GYE	1	4 Virtual Processors Intel(R) Xeon(R) CPU E5-2690 0 @ 2.90GHz 8 GB RAM	Microsoft Windows Server 2012 R2 (64-bit)	Servidor Virtual
Servidor consola de Antivirus SEP	1	2 Virtual Processors Intel(R) Xeon(R) CPU E5-2690 0 @ 2.90GHz 8 GB RAM	Microsoft Windows Server 2012 R2 (64-bit)	Servidor Virtual

Fuente: Subsecretaría de Innovación de las Finanzas Públicas
Elaboración: Dirección Nacional de Operaciones

Todos estos elementos han soportado la ejecución de las diferentes transacciones de negocio en los diferentes sistemas de gestión de las finanzas públicas: e-SIGEF, SPRYN, eByE y SIGADE, junto con sus interoperabilidades.

2.2 Identificación, descripción y diagnóstico del problema

2.2.1 Definición del Problema

Elevado riesgo en la prestación de servicios del Ente Rector a las entidades del sector público no Financiero, relacionado a la gestión de las finanzas públicas por la desactualización de la infraestructura tecnológica.

2.2.2 Causas

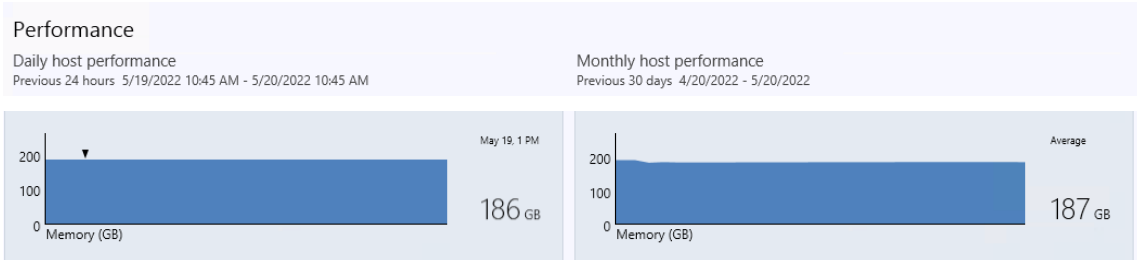
Al tener una plataforma tecnológica desactualizada se tienen las siguientes causas:

- Brechas en sistemas informáticos del Ente Rector. Existe una limitación en el crecimiento tecnológico en las aplicaciones actuales del Sistemas de las Finanzas Públicas tanto en su capacidad, como en la posibilidad de cerrar brechas de seguridad de sus sistemas o de su entorno, y proporcionar la disponibilidad del servicio que las entidades públicas requieren para un sistema transaccional de gestión financiera. Esta brecha existe debido a los avances tecnológicos de los últimos años, y la imposibilidad de avanzar con una infraestructura acorde a las necesidades tecnológicas actuales.

- Infraestructura obsoleta, sin garantía y soporte. El Ministerio de Economía y Finanzas tiene actualmente infraestructura tecnológica cuya fecha de fin de vida útil ya fue declarada por parte de sus fabricantes, la misma ya se cumplió o está por cumplirse en los siguientes meses, de acuerdo a comunicaciones formales recibidas por parte de los fabricantes del hardware.
  El concepto dado por los fabricantes de hardware de la vida útil de un equipo, es el fin de soporte extendido sobre el equipamiento, es decir, ya no se fabricaran los modelos de los equipos cuyo tiempo de vida útil finalizó, tampoco se construirán partes y piezas de repuesto, y no se generarán más actualizaciones de microcódigo o firmware requerido para operar adecuadamente el equipo y cerrar brechas de seguridad; por tanto, no hay el soporte para mantener disponible el equipo en caso de una incidencia.
  Esta Cartera de Estado posee actualmente un porcentaje importante de equipos que tienen más de ocho años de antigüedad y como ya se ha indicado han cumplido su vida útil, la consecuencia de esto es que no se dispone de soporte y garantías directamente de fábrica, ya no se construyen equipos para reemplazo o repuestos y tampoco se generan nuevas versiones de sistemas operativos o microcódigo para su mejor funcionamiento o cierre de brechas de seguridad

- Limitada capacidad de crecimiento.

  La infraestructura física que soporta la Nube privada, se encuentra utilizada en un 93% de su capacidad, lo que limita la generación de nuevas máquinas virtuales o el reforzamiento de las existentes; esto impacta directamente en el servicio de las aplicaciones por cuanto no se tienen la posibilidad de aumentar su capacidad para acceso de más usuarios o produce lentitud en la generación de nóminas grandes. A continuación, la gráfica de monitoreo de la capacidad de la Nube:



Fuente: Subsecretaría de Innovación de las Finanzas Públicas
Elaboración: Dirección Nacional de Operaciones

Limita también la posibilidad de utilizar nuevas funcionalidades y bondades que la nueva versión del sistema operativo Windows 2019 o 2022 y el virtualizador System Center 2019 o 2022, que son las herramientas que permiten la creación de una Nube privada. El riesgo existente es que ante cualquier incidente o falla que se presente, este no pueda solventarse con el soporte del fabricante por las versiones no vigentes, lo que podría ocasionar degradación en su servicio, acceso limitado a los usuarios o suspensiones de servicio en las aplicaciones.

La inadecuada infraestructura física afecta también los procesos de generación de respaldos de la información y configuración de las aplicaciones del Ente Rector, actividad que es una buena práctica tecnológica y además necesaria para garantizar la disponibilidad de la información en caso de un incidente tecnológico no deseado o por necesidad institucional.

Los procesos de generación y copia de respaldos de la información de las aplicaciones que permiten la gestión de las finanzas pública de las entidades del sector no financiero y que pertenecen al Presupuesto General del estado (“PGE”) toman demasiado tiempo que no es ni eficiente ni óptimo debido a que se utilizan plataformas con tecnología de más de 8 años.

Existen nuevas tecnologías para la gestión y administración de respaldos que no pueden ser aplicadas debido a las limitaciones tecnológicas propias de la actual plataforma e infraestructura de respaldos.

2.2.3 Consecuencias o efectos

Costos elevados de mantenimiento de hardware y dificultad en encontrar partes y piezas.

En el año 2010 se realizó un proyecto de reforzamiento tecnológico cuyo alcance fue:

- Implementación de Equipos de comunicación, switches, que mejoraron la interconexión entre redes y ampliaron el ancho de banda para las comunicaciones.
- Equipos para la seguridad perimetral, que permitieron gestionar mecanismos e implementar controles para asegurar el acceso de los usuarios a los sistemas.
- Equipos para el balanceo de carga generada por las aplicaciones y los enlaces de comunicación
- Sistema de almacenamiento
- Servidores con tecnología RISC
- Equipamiento para los respaldos de información: librería virtual de cintas (VLS 12000) y librería física de cintas ESL-322e con tecnología de drives LTO4, y el software de gestión de respaldos.

Año 2013 se adquirió 2 chasis C7000 y 16 servidores para la implementación de la nube privada para actualizar la tecnología de los servidores y aplicaciones del Sistema Nacional de las Finanzas Públicas.

Año 2017 se contrató infraestructura tecnológica para fortalecer el Sistema Nacional de las Finanzas Públicas, la misma que consistía en el fortalecimiento de los servidores de Base de Datos de Producción HP Integrity SuperDome2, implementación del sistema de almacenamiento HP 3PAR 20450 y SAN Directores como la integración del SWITCH CORE LAN HP – ARUBA con el SWITCH CORE LAN CISCO SYSTEMS WS-C6509-E.

Luego de finalizada la garantía, se han realizado contratación de renovación del soporte y garantía, en la que se evidencia el crecimiento en los costos, lo que se describe en la siguiente tabla:

Tabla 12 Costos de los contratos de renovación del soporte y garantía de la infraestructura

Año	Costos de mantenimiento ()
14/05/2015 - 14/05/2016	394.900,00
15/05/2016 - 15/05/2017	563.000,00
01/07/2017 - 31/12/2017	231.589,00
05/02/2018 - 05/02/2019	528.554,96
14/02/2019 -14/02/2020	530.000,00
15/02/2020 - 15/02/2021	539.000,00
10/05/2021 - 10/05/2022	554.399,00
10/05/2022 - 10-05-2023	805.000,00

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo gestión del proyecto

En relación a los repuestos y partes y piezas para actualizar la plataforma cuyo tiempo de vida útil esta vencido o próximo a vencer, se dificulta su obtención es más costos y en muchas ocasiones ya no existen.

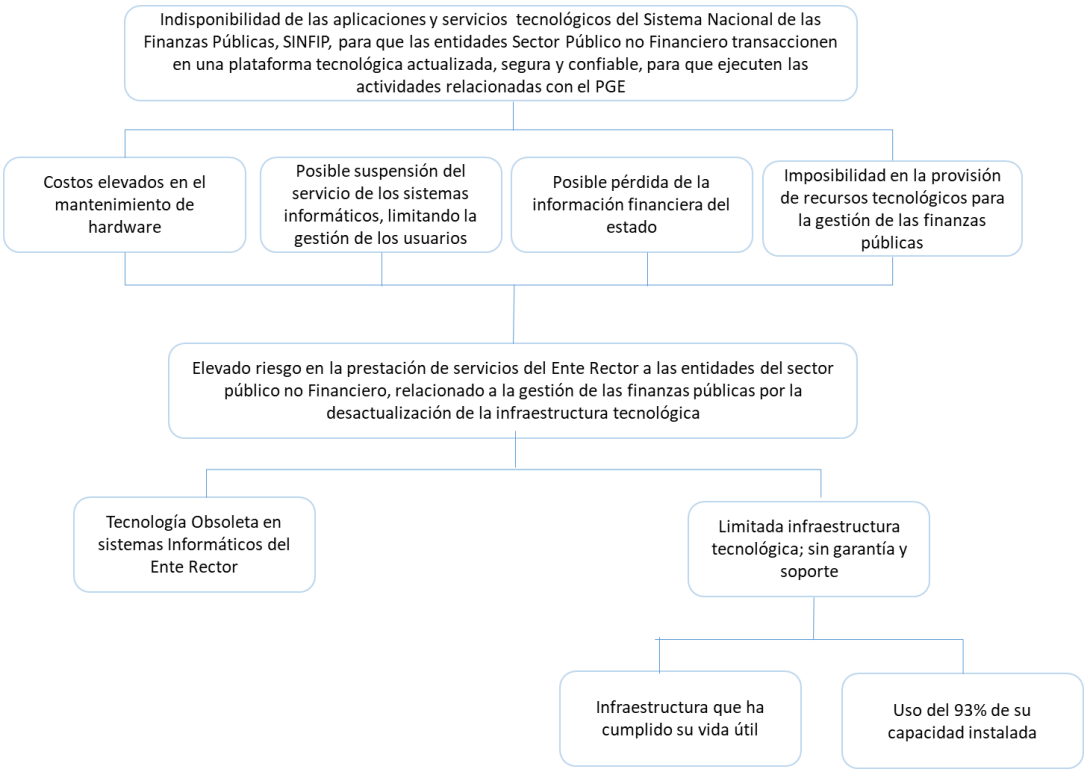
- Posible suspensión del servicio de los sistemas informáticos, limitando la gestión de los usuarios. Una consecuencia directa de no tener una plataforma actual, con tecnología vigente es la alta probabilidad de que este equipamiento sufra daños físicos y no tener la posibilidad de ponerlo operativo en tiempos adecuados, por falta de repuestos, lo que afectaría directamente al servicio de las aplicaciones del Sistema de las Finanzas Públicas por ende a la gestión financiera que las entidad y usuarios realizan en estas aplicaciones.
- Posible pérdida de la información financiera del estado. De existir daño en los equipos responsables del sistema de respaldos, afectaría directamente a la posibilidad de generar respaldos diarios de la información transaccional de las aplicaciones, y por ende a la pérdida de la información de presentarse incidencias; además la limitación de no poder entregar información histórica a las diferentes entidades u entes de control.
- Imposibilidad en la provisión de recursos tecnológicos para la gestión de las finanzas públicas, por la falta de capacidad tecnológica de la plataforma que soporta a las aplicaciones ya que se encuentra al límite, restringe la entrega de recursos ya sea para reforzar la capacidad transaccional en tiempos picos de acceso de usuarios o de número de transacciones, o para atender nuevas necesidades tecnológicas del Ente Rector.

2.2.4 Efecto final

La problemática que implica el tener una infraestructura tecnológica desactualizada que no cubre las necesidades del Ente Rector y sus procesos financieros, tiene el efecto final de:
La falta de capacidad para mantener la disponibilidad y continuidad de las aplicaciones y servicios tecnológicos del Sistema Nacional de las Finanzas Públicas, SINFIP, para que las entidades Sector Público no Financiero transacciones en una plataforma tecnológica actualizada, segura y confiable, para que ejecuten las actividades relacionadas con el PGE

2.2.5 Árbol de Problemas

Para identificar de una mejor manera lo expuesto a continuación el árbol del problema:



Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo gestión del proyecto

2.3 Línea base del proyecto

El Ministerio de Economía y Finanzas como Ente Rector de las finanzas públicas brinda a las instituciones del sector público, el servicio de las aplicaciones tecnológicas: eSIGEF, SPRYN, Bienes y Existencias, Interoperabilidades, el Sistema de Gestión y Análisis de Deuda SIGADE, entre las principales; para mantener su disponibilidad y continuidad de los servicios de las aplicaciones antes indicadas, esta Cartera de Estado ha realizado inversiones en su infraestructura y plataforma tecnológica a lo largo de los años, para cubrir y solventar las diferentes necesidades tecnológicas.

Para la elaboración de línea base se recolectó la información que enmarca los ámbitos de la gestión del Sistema Nacional de las Finanzas Públicas, dicha la información evidencia el estatus y datos que reflejan la situación tecnológica actual.

Para la consolidación de los distintos parámetros de información que fue considerada para desarrollar este análisis, se enfocará en los usuarios aprobadores de las entidades del Presupuesto General del Estado que transaccional en los Sistemas de las Finanzas Públicas, equivalentes a 6420 usuarios que poseen las funciones de aprobador que intervienen en el proceso crítico de pagos.

Como insumo del presente proyecto, a continuación, se describen varios estudios, análisis de situación y datos, para determinar la línea base de infraestructura tecnológica:

2.3.1 Estudio de Brechas Tecnológicas

El Ministerio de Economía y Finanzas a través de la Dirección Nacional de Operaciones de los Sistemas de las Finanza Públicas, con fecha el 20 de mayo de 2022 emite un informe de la situación actual de la infraestructura tecnológica del Centro de Datos Principal, misma que soporta a los Sistemas de las Finanzas Públicas, concluyendo que:

Los equipos de comunicaciones y seguridad: nube, sistema de respaldos, balanceadores, firewalls y switches, han cumplido o están **próximos** a cumplir su tiempo de vida útil, declarado por sus propios fabricantes, esto lleva a tener un alto riesgo de ser vulnerados, por tener versiones desactualizadas de sistemas operativos, no poder instalar actualizaciones y parches que corrijan fallas de funcionamiento y seguridad; que solventen todas las potenciales amenazas que se encuentran en los boletines y alertas que regularmente los fabricantes informan. Adicionalmente, el riesgo se extiende a su disponibilidad, por cuanto los repuestos de partes y piezas ya no están siendo fabricados por cuanto llegará un momento que no existan reemplazo de piezas dañadas

2.3.2 Estudio de Infraestructura Tecnológica

La Dirección Nacional de Operaciones de los Sistemas de las Finanzas Públicas, emite un informe de Justificación Técnica Motivada de la necesidad, en el cual se realiza un estudio de situación actual de la infraestructura, del que se puede destacar los siguientes puntos:

La información que esta Cartera de Estado administra es altamente sensible por lo que se tiene que garantizar la seguridad y alta disponibilidad de las misma, las principales aplicaciones de los Sistemas de las Finanzas Públicas actualmente soportadas, son:

- Sistema Administrativo Financiero (eSigef)
- Sistema Presupuestario de Remuneraciones y Nómina (SPRYN)
- Bienes&Existencias
- Sistema de Manejo de Deuda (SIGADE)
- Business Intelligence (BI).
- Aplicaciones Internas

Los equipos de seguridad perimetral, balanceadores de carga que actualmente posee el MEF según lo indicado por los fabricantes de los mismos, han cumplido con su vigencia tecnológica por lo que es necesario su reemplazo. Lo mismo sucede con la infraestructura tecnológica de Respaldos.

2.3.3 Informe de disponibilidad de los servicios de tecnología, durante el periodo (agosto) del 2022

La Dirección Nacional de Operaciones de los Sistemas de las Finanzas Públicas, emite el Informe de Disponibilidad de los servicios de tecnología, correspondiente al periodo del 01 al 31 de agosto del 2022, el mismo que muestra el porcentaje de disponibilidad total de los servicios de tecnología, mismo que es un compendio de la disponibilidad de todos sus componentes, y se establece un porcentaje de **99.98**%.

A continuación, se describe el porcentaje de disponibilidad del servicio de infraestructura tecnológica durante el año 2022:

Tabla 13 Disponibilidad del servicio de infraestructura tecnológica

Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto
99,98%	99,98%	99,98%	99,97%	99,97%	99,97%	99,98%	99,98%

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP

Elaboración: Equipo gestión del proyecto

2.3.4 Información de levantamiento tecnológico del MEF

En el mes de agosto de 2022 se realiza un levantamiento del inventario de todo el hardware, de ese resultado se tiene que, de los 128 equipos obtenidos del levantamiento, con una ponderación del tiempo de vida útil y la criticidad del equipo, da como resultado el 48% de obsolescencia del equipamiento.

Tabla 14 Obsolescencia de la infraestructura

Año	2022
% de obsolescencia	48%

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaboración: Equipo gestión del proyecto

2.3.5 Informe de estado actual de la Base de Datos transaccional

En agosto del 2022, la Dirección Nacional de Operaciones de los Sistemas de las Finanzas Públicas emite un *Informe del estado actual de la Base de Datos Transaccional* de las aplicaciones del sistema de las Finanzas Públicas, luego de una migración de versión de la Base de datos 11.2. 0.4 (11g) a la versión 19c; misma que ofrece funcionalidades nuevas en la gestión mejoras en el rendimiento, escalabilidad, fiabilidad y seguridad. Además, proporciona el nivel más alto de estabilidad de la versión y el marco de tiempo más largo en cuanto a soporte y correcciones de errores.

2.3.6 Detalle de Nivel de Capacitación Tecnológica recibida

Con referencia *Detalle de Nivel de Capacitación Tecnológica* recibida a los funcionarios que son responsables de la administración de la plataforma tecnológica que soporta las aplicaciones de los sistemas de gestión de las finanzas públicas, en estos dos últimos años, se puede determinar que solo 44.44% del personal ha recibido capacitaciones de tecnología actualizada, como se detalla en la siguiente tabla:

Tabla 15 Capacitaciones y funcionarios capacitados en tecnologías actualizadas

Denominación	No. Servidores
HM9Q1S: HPE SAN Essentials I: Administration Fundamentals	4
HM9Q2S: HPE SAN Essentials II: Advanced B-series Networking	4
HK766S: Managing HPE StoreOnce Backup Solutions	4
AZ-900 Azure Fundamentals	4

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaboración: Equipo gestión del proyecto

2.3.7 Infraestructura tecnológica obsoleta

En cuanto a la *Infraestructura tecnológica obsoleta* se parte de un análisis de la totalidad del equipamiento que posee el Ministerio de Economía y Finanzas, mismo que muestra que el equipamiento que ha cumplió su vida útil o está próximo a vencerse, además de que el soporte a los equipos por parte de los fabricantes está llegando a la fecha fin de su cobertura. Se tiene como resultado que del 100% de la infraestructura, existe un porcentaje del 48%; esto provoca una afectación colateral además de la infraestructura, se afecta al software base, imposibilitando su actualización por no tener un hardware que soporte las últimas versiones; en el corto plazo dando como resultado una operación inadecuada, imposibilidad de cerrar nuevas brechas de seguridad y afectación al servicio.

2.3.8 Usuarios del PGE relacionados con Infraestructura tecnológica

Para la determinación de la línea base un punto importante de análisis son los usuarios de los sistemas que son parte de las entidades del Presupuesto General del Estado y que por esta condición dependen de la infraestructura tecnológica.

En la siguiente Tabla se muestra la variación de los diferentes elementos que intervienen en la gestión de la administración financiera pública, como: número de entidades públicas, los usuarios que transaccional en el Sistema Nacional de las Finanzas Públicas con las funciones de aprobador y el número de servidores públicos del Presupuesto General del Estado en el periodo 2018 a 2022.

Tabla 16 Cantidad de usuarios PGE relacionados con la infraestructura tecnológica

Denominación	Situación actual				
	2018	2019	2020	2021	2022
Nro. Entidades PGE	1.243	1.232	1.325	1.237	1.032
Nro. Usuarios PGE	3.925	3.496	5.626	8..140	11.290
Nro. Usuarios Funciones Aprobador	12.032	11.914	1.956	4379	6.420
Nro. Servidores Públicos PGE	537.581	525.936	483.211	481.394	481.979

Fuente: Subsecretaría de Innovación de las Finanzas Públicas
Elaboración: Equipo gestión del proyecto

2.3.9 Nivel de satisfacción de los Usuarios

Un punto importante a ser analizado para la línea base es el *Nivel de satisfacción de los Usuarios*. En la siguiente tabla se muestra el cuadro de Nivel de Satisfacción de los Usuarios que evidencia la evolución de la aceptación de la operatividad del Sistema Nacional de las Finanzas Públicas desde el periodo de 2018 al 2022.

Tabla 17 Nivel de satisfacción de usuarios relacionados con la infraestructura tecnológica

Denominación	Situación actual				
	2018	**2019**	**2020**	**2021**	**2022**
Usuarios	83%	78%	70%	73%	85%

Fuente: Subsecretaría de Innovación de las Finanzas Públicas
Elaboración: Equipo gestión del proyecto

2.3.10 Obsolescencia de los equipos tecnológicos

La siguiente tabla detalla la *Obsolescencia de los equipos tecnológicos* que explica el incremento de la obsolescencia de la plataforma tecnológica de análisis en los últimos cinco años.

Tabla 18 Obsolescencia de la infraestructura tecnológica

Denominación	Situación actual				
	2018	**2019**	**2020**	**2021**	**2022**
Nube	30%	45%	60%	75%	90%
Sistema respaldo	70%	85%	100%	100%	100%
Balanceador	0%	25%	45%	65%	85%
Switch	15%	30%	45%	100%	100%
Firewall	25%	100%	100%	100%	100%
				PROMEDIO	**95%**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas
Elaboración: Equipo gestión del proyecto

2.3.11 Análisis de probabilidad de falla de los equipos tecnológicos

La siguiente tabla, muestra la *Probabilidad de falla de funcionamiento de infraestructura tecnológica* desde el periodo de 2018 al 2022, el análisis se realiza al equipamiento que soporta al Sistema Nacional de las Finanzas Públicas, el resultado de probabilidad de falla a la fecha es 76%.

Tabla 19 Probabilidad de falla de funcionamiento de infraestructura tecnológica

Denominación	Situación actual				
	2018	2019	2020	2021	2022
Nube	80%	80%	80%	80%	80%
Sistema respaldo	80%	80%	80%	80%	80%
Balanceador	35%	50%	65%	80%	80%
Switch	45%	60%	75%	80%	80%
Firewall	20%	50%	60%	60%	60%
				PROMEDIO	**76%**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas
Elaboración: Equipo gestión del proyecto

2.3.12 Impacto en el caso de falla en el funcionamiento de la infraestructura tecnológica

La Tabla 20 muestra el *Impacto falla de funcionamiento de infraestructura tecnológica* el cual indica la magnitud de la afectación en caso de falla de los equipos que conforman la operatividad del Sistema Nacional de las Finanzas Públicas, el análisis se realiza desde el periodo de 2018 al 2022.

Tabla 20 Impacto falla de funcionamiento de infraestructura tecnológica

Denominación	Situación actual				
	2018	2019	2020	2021	2022
Nube	1,00	1,00	1,00	1,00	1,00
Sistema respaldo	0,80	0,80	0,80	0,80	0,80
Balanceador	0,80	0,80	0,80	0,80	0,80
Switch	1,00	1,00	1,00	1,00	1,00
Firewall	1,00	1,00	1,00	1,00	1,00

Fuente: Subsecretaría de Innovación de las Finanzas Públicas
Elaboración: Equipo gestión del proyecto

2.3.13 Riesgo de falla en el funcionamiento de la infraestructura tecnológica

A continuación, se define el *Riesgo de falla en el funcionamiento de la infraestructura tecnológica*, tomando en consideración la probabilidad y el impacto. En la siguiente tabla se muestra el cuadro de resultado del riesgo de funcionamiento de infraestructura tecnológica en porcentaje y analizado desde el periodo de 2018 al 2022.

Tabla 21 Riesgo de funcionamiento de infraestructura tecnológica

Denominación	Situación actual				
	2018	2019	2020	2021	2022
Nube	80%	80%	80%	80%	80%
Sistema respaldo	64%	64%	64%	64%	64%
Balanceador	28%	40%	52%	64%	64%
Switch	45%	60%	75%	80%	80%
Firewall	20%	50%	60%	60%	60%

Fuente: Subsecretaría de Innovación de las Finanzas Públicas
Elaboración: Equipo gestión del proyecto

2.3.14 Disponibilidad de los servicios tecnológicos

La disponibilidad como concepto es la continuidad operacional durante un período de medición dado. El tiempo de disponibilidad se mide con el tiempo de inactividad. De acuerdo a lo indicado en ITIL1, la disponibilidad es el porcentaje de tiempo sobre el total acordado en que los servicios TI han sido accesibles al usuario y han funcionado correctamente.

El indicador, porcentaje de disponibilidad, pretende mostrar el resultado de la división del tiempo que el servicio, plataforma, infraestructura de producción, etc., se encuentra operativo sobre el período de tiempo total definido para el análisis.

La Tabla 22 muestra la información relacionada a la *Disponibilidad de los servicios* que ofrece el Ministerio de Economía y Finanzas en porcentaje y refleja la operatividad en línea de los Sistema Nacional de las Finanzas Públicas en el presente año.

Tabla 22 Disponibilidad de Servicios que ofrece el MEF

Denominación	% Disponibilidad
Sistema Integrado de Gestión Financiera - (eSIGEF	99,99%
Subsistema Remuneraciones y Nómina - (SPRYN)	99,98%
Bienes y Existencias - (eByE)	99,99%
Sistema Remuneraciones y Nómina - (eSIPREN)	99,99%
PROMEDIO	**99,99%**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaboración: Equipo gestión del proyecto

[1] ITIL, (InformationTechnologyInfrastructure Library), es una colección de las mejores prácticas observadas en la industria de TI convirtiéndose en un estándar para la administración de los servicios de tecnología de información hacia las organizaciones.

2.3.15 Vigencia del soporte y garantía de la infraestructura tecnológica

La Tabla 23 muestra el cuadro de *Vigencia de Soporte y Garantía de infraestructura tecnológica* en el que se muestra la información del estado de soporte y garantía del equipamiento por parte de los fabricantes. La garantía y soporte permite en caso de presentarse incidentes o errores tener la posibilidad de solventarlos en tiempos adecuados, y en el caso de fallos en las partes y piezas de los mismos, se tengan los repuestos de reemplazo y así lograr la operatividad de los equipos y su servicio. El análisis se realiza en el periodo de 2018 al 2022, y a la presente fecha se tiene un 20% de los equipos que posee soporte y garantía con el fabricante, del equipamiento en análisis.

Tabla 23 Vigencia del soporte de la infraestructura tecnológica

Situación actual										
Denominación	2018		2019		2020		2021		2022	
	X	Y	X	Y	X	Y	X	Y	X	Y
Nube	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
Sis. Respaldo	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
Balanceador	Si	Si	No	Si	No	Si	No	Si	No	No
Switch	Si	Si	Si	Si	No	No	No	No	No	No
Firewall	No	No	No	No	No	No	No	No	No	No

Fuente: Subsecretaría de Innovación de las Finanzas Públicas
Elaboración: Equipo gestión del proyecto

X: Soporte *Y: Garantía*

2.3.16 Resumen de Línea Base

A continuación, en la tabla 24 se tiene el cuadro resumen de *Línea Base* con los resultados de los indicadores reportados relevante del presente proyecto y obtenidos en el año 2022.

Tabla 24 Resumen indicadores considerados para la línea base

Denominación	2022
Estudios de Brechas Tecnológicas	1
Estudios de Situación Actual de Infraestructura	4
% de funcionarios de la DNOSFP capacitados en tecnologías	44%
% de Satisfacción de usuarios relacionados con la infraestructura tecnológica	85%
% Disponibilidad del servicio de infraestructura tecnológica	99,98%
Nro. Entidades PGE	1.032

Denominación	2022
Nro. Usuarios PGE	11.290
No. Usuarios Funciones Aprobador	6.420
Nro. Servidores Públicos PGE	481.979
Obsolescencia del 100% infraestructura tecnológica	48%
% de Probabilidad de falla de funcionamiento de infraestructura tecnológica	76%
% de Impacto falla de funcionamiento de infraestructura tecnológica	92%
% de Riesgo de funcionamiento de infraestructura tecnológica	70%

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Dirección Nacional de Operaciones

2.4 Análisis de oferta y demanda

El Ministerio de Economía y Finanzas es el Ente Rector de las Finanzas Públicas, por este rol, proporciona los servicios de las aplicaciones tecnológicas que permite la gestión de las finanzas públicas además de que es la principal fuente de la información resultante de esta gestión.

2.4.1 Oferta

En el artículo 175 del Código Orgánico de Planificación y Finanzas Públicas entrega al ente rector de las finanzas públicas la potestad de establecer un sistema oficial de información:

"El ente rector de las finanzas públicas deberá establecer un sistema oficial de información y amplia difusión que servirá de base para el control de la Función Legislativa, así como de la ciudadanía, (…)"

Asimismo, que los gobiernos autónomos descentralizados, las entidades a cargo de la seguridad social, las empresas públicas y la banca pública establecerán sus propios sistemas, debiendo consultar mecanismos para la remisión de información al ente rector para fines de consolidación, como también que incluirán la información sobre lo dispuesto en el código y en la legislación vigente.

En la disposición general decima segunda del Código Orgánico de Planificación y Finanzas Públicas, se determina que las transacciones financieras realizadas entre entidades del Presupuesto General del Estado se las realizará a través de la plataforma informática del sistema de administración financiera, las mismas que permitirán realizar todos los procesos en medio digitales, sin requerir soportes físicos adicionales.

Los servicios que presta el Ministerio de Economía y Finanzas son:

Tabla 25 Servicios informáticos del Ente Rector

Servicios Informáticos
Sistema de Gestión y Análisis de la Deuda (SIGADE)
Sistema de Monitoreo de Servicios e Infraestructura (SCOM)
Gestión de Incidentes (SCSM)
Sistema de Despliegue de Parches (SCCM)
Gestión del ciclo de vida del desarrollo (Azure Devops Server)
Sitio de colaboración documental (Sharepoint Foundation)
Inteligencia de Negocio (COGNOS)
Servicio de generación de reportes de Inteligencia de Negocio (BI REPOSITORIO)
Servicio de Publicación de reportes de Inteligencia de Negocio (BI NextCloud)
Sistema de Reportería (ADA)
Sistema de Respaldos
Symantec Endpoint Protection (SEP)
Sistema de Autenticación Biométrica para pagos Presupuestarios y Contables
44 Interoperabilidades (Servicios Web y Replicas de BDD)
Sistema Integrado de Gestión Financiera - (eSIGEF)
Subsistema Presupuestario de Remuneraciones y Nómina - (SPRYN, eSIPREN)
Sistema de Bienes y Existencias - (eByE)

Fuente: Subsecretaría de Innovación de las Finanzas Públicas
Elaboración: Dirección Nacional de Operaciones

2.4.2 Demanda

En el artículo 225 de la Constitución de la República, se enumera la conformación del sector público en términos que comprende:

- Los organismos y dependencias de las funciones Ejecutiva, Legislativa, Judicial, Electoral y de Transparencia y Control Social.
- Las entidades que integran el régimen autónomo descentralizado.
- Los organismos y entidades creados por la Constitución o la ley para el ejercicio de la potestad estatal, para la prestación de servicios públicos o para desarrollar actividades económicas asumidas por el Estado.
- Las personas jurídicas creadas por acto normativo de los gobiernos autónomos descentralizados para la prestación de servicios públicos.

El mismo cuerpo legal, en los artículos 297 y 315, agrega que las instituciones y entidades que reciban o transfieran bienes o recursos públicos se someterán a las normas que las regulan y a los principios y procedimientos de transparencia, rendición de cuentas y control público. Como también que las empresas públicas estarán bajo la regulación y el control específico de los organismos pertinentes, de acuerdo con la ley; funcionarán como sociedades de derecho público, con personalidad jurídica, autonomía financiera, económica, administrativa y de gestión, con altos parámetros de calidad y criterios empresariales, económicos, sociales y ambientales.

2.4.3 Población de referencia

Existen a nivel país, en el Estado el siguiente volumen de instituciones que potencialmente podrían usar el sistema:

Tabla 26 Entidades potenciales para usar el sistema

Sector	Nombre de Sector	No. Entidades
111	Administración del Estado	960
112	Entidades de Educación Superior	65
113	Entidades de Seguridad Social	105
121	Gobiernos Autónomos Descentralizados Provinciales	45
122	Gobiernos Autónomos Descentralizados Municipales	711
123	Gobiernos Autónomos Descentralizados Parroquiales	863
211	Empresas Publica de la Función Ejecutiva	54
212	Empresas Publicas de los GADS	261
221	Entidades Financieras Publicas	13
311	Sociedades Anónimas con Participación Públicas	22
	Total Entidades	**3,099**

Fuente: Ministerio de Finanzas e-SIGEF- Corte agosto 2022
Elaborado por: Equipo gestión del proyecto

2.4.4 Población demandante Potencial

La población demandante potencial que podría acceder al servicio, la constituyen los usuarios activos de los sistemas del Ente Rector, esto es 11.290 usuarios.

2.4.5 Población demandante Efectiva

La población demandante efectiva la constituyen los usuarios de los sistemas del Ente Rector, que participan en el proceso de pagos, uno de los procesos más críticos y demandados de las instituciones que pertenecen al Presupuesto General del Estado, y son 6.420. Esta es la población que se atenderá hasta finalizar la ejecución del proyecto.

2.4.6 Estimación del Déficit o Demanda Insatisfecha

Al ser una actualización tecnológica de la plataforma que soporta a las aplicaciones del ente rector y que son utilizadas por todas las entidades dentro del PGE, para sus procesos de gestión financiera pública. La demanda insatisfecha constituye en realidad la misma oblación demandante efectiva constituida por los usuarios de las entidades que participan en el PGE y que están obligadas a utilizar el sistema. Es decir, la demanda insatisfecha son los 6.420 usuarios.

2.5 Identificación y Caracterización de la población objetivo

De acuerdo a lo establecido en la COPLAFIP todas las instituciones y organismos comprendidos en los artículos 225, 297 y 315 de la Constitución de la República se sujetarán al SINFIP. Los principales beneficiarios de este programa son las entidades e instituciones, que integran el Sector Público Ecuatoriano, niveles gerenciales, administrativos, contables, financieros y operativos, que utilizan o se incorporan en diferentes fases al Sistema de Administración Financiera, quienes lograrán:

- Alcanzar la modernización del Estado con instituciones ágiles y eficientes.
- Acceso en forma oportuna a la información de calidad de las finanzas públicas, que permitan un mejorar el proceso de toma de decisiones.
- Fiscalizar inteligente y coordinadamente la ejecución presupuestaria por parte de los servicios públicos y los órganos contralores.
- Agregar y segmentarlos ejercicios presupuestarios por diversas dimensiones, variables y ejes.
- Optimizar los recursos, tanto humanos como materiales.
- Obtener un instrumento de apoyo para la gestión pública
- Mejorar el control de las operaciones y transacciones.

En concordancia a la línea base y al segmento de usuarios en estudio, se selecciona 6420 usuarios del PGE perteneciente a Instituciones del SPNF, estos usuarios tienen asignadas funciones en el sistema eSIGEF para realizar operaciones de aprobación de transacciones.

A partir de los 6420 usuarios aprobadores se puede segmentar por módulo del Core del negocio, determinándose las necesidades de operar por módulo.

Tabla 27 Cantidad de usuarios aprobadores por módulo

Módulos	Número Usuarios
Aprobador Contabilidad	1,796
Aprobador Nómina	1,250
Aprobador Presupuesto	1,427
Aprobador Tesorería	1,472
Aprobador Adm. Usuarios	475
Total general	**6420**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNCS

Elaboración: Equipo gestión del proyecto

Adicionalmente, se realiza el análisis del segmento de usuarios aprobadores por provincia, evidenciando la cantidad de usuarios que transaccional en cada provincia.

Tabla 28 Cantidad de usuarios PGE que usan el aplicativo por provincia

Situación actual	Usuarios Aprobadores
AZUAY	211
BOLIVAR	100
CANAR	105
CARCHI	87
CHIMBORAZO	148
COTOPAXI	115
EL ORO	196
ESMERALDAS	152
GALAPAGOS	84
GUAYAS	843
IMBABURA	148
LOJA	223
LOS RIOS	160
MANABI	373
MORONA SANTIAGO	105
NAPO	88
ORELLANA	163
PASTAZA	96
PICHINCHA	2,574
SANTA ELENA	96
SUCUMBIOS	78
TUNGURAHUA	195
ZAMORA CHINCHIPE	80
Total general	**6420**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNCS

Elaboración: Equipo gestión del proyecto

2.6 Ubicación geográfica e impacto territorial

El proyecto implica una ejecución gubernamental de impacto nacional con la administración y ubicación física en el Ministerio de Economía y Finanzas en la ciudad de Quito. La actualización tecnológica a la plataforma de los sistemas que gestionan las finanzas públicas estará ubicada en la ciudad de Quito, los usuarios que acceden al sistema y lo utilizan pertenecen a las entidades que operan a nivel nacional.

3. ARTICULACIÓN CON LA PLANIFICACIÓN

3.1 Alineación objetivo estratégico institucional

El proyecto de Actualización tecnológica para el fortalecimiento de las finanzas públicas, está alineado al siguiente objetivo:

- Objetivo Estratégico Institucional: Incrementar la eficacia, eficiencia, calidad y transparencia en la gestión de ingresos, egresos y financiamiento del sector público.

Tabla 29 Alineación objetivo estratégico Institucional

Indicador	Meta 2023	Meta 2024
Porcentaje de implementación de nuevas funcionalidades del SINFIP	96,00%	97,00%

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo gestión del proyecto

3.2 Contribución del proyecto a la meta del Plan Nacional de Desarrollo – Plan de Creación de Oportunidades 2021-2025 de Ecuador

El proyecto de Actualización tecnológica para el fortalecimiento de las finanzas públicas se encuentra alineada al Plan de Creación de Oportunidades 2021-2025 de Ecuador en:

–Eje: Económico

- Objetivo 4: Garantizar la gestión de las finanzas públicas de manera sostenible y transparente.

Políticas del Plan Nacional de Desarrollo:

- 4.5. Generar condiciones macroeconómicas óptimas que propicien un crecimiento económico inclusivo y sostenible

Meta:

- 4.5.1 Alcanzar superávit de SPNF a 2025 de 0.35% del PIB.

4. MATRIZ MARCO LÓGICO

4.1 Objetivo General y Objetivos Específicos

4.1.1 Objetivo General

Actualizar la infraestructura tecnológica del Ministerio de Economía y Finanzas cuyo tiempo de vida útil terminó o está por terminar, necesaria para la prestación eficiente de los servicios al sector público no Financiero.

4.1.2 Objetivos Específicos

Para concretar el objetivo general planteado en el proyecto de actualización tecnológica de la plataforma, se deben cumplir con los siguientes objetivos específicos:

- Fortalecer la infraestructura tecnológica de la Cartera de Estado
- Reducir la brecha tecnológica y operativa del Ministerio de Economía y Finanzas.

Con lo cual se pretende:

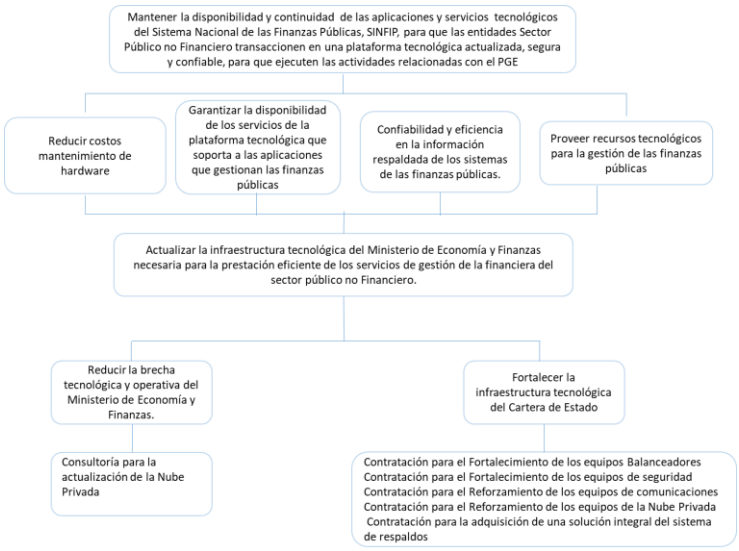
- Reducir los costos de mantenimiento de hardware, ya que se tendrá una plataforma actualizada y con garantía vigente.
- Garantizar la disponibilidad de los servicios de la plataforma tecnológica que soporta a las aplicaciones que gestionan las finanzas públicas, teniendo una infraestructura confiable y actualizada y una Nube Privada con la última versión estable.
- Confiabilidad y eficiencia en la información respaldada de los sistemas de las finanzas públicas, ya que se tendrá un sistema de respaldos de última tecnología y que permita optimizar el tiempo requerido para obtener los respaldos de información de los sistemas, además de salvaguardar de mejor manera la información histórica con nuevas seguridades y contingencia.

- Proveer recursos tecnológicos para la gestión de las finanzas públicas, para cubrir las necesidades del Ente Rector relacionadas a capacidades tecnológicas para la ejecución de sus procesos de negocios y el de las entidades que utilizan los sistemas.

Finalmente, con la ejecución del proyecto se mantendrá la disponibilidad y continuidad de las aplicaciones y servicios tecnológicos del Sistema Nacional de las Finanzas Públicas, SINFIP, para que las entidades del Sector Público no Financiero transacciones en una plataforma tecnológica actualizada segura y confiable, ejecutando las actividades relacionadas a este ámbito en el PGE.

4.1.3 Árbol de Objetivos

A continuación, se describe el Árbol de Objetivos:



Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo gestión del proyecto

4.2 Indicadores de resultado

Se ha identificado y determinado los indicadores de resultado para el proyecto, en el marco de los objetivos y componentes, con la finalidad de reflejar el impacto dentro del Ministerio a través de la Subsecretaría de Innovación de las Finanzas Públicas, a continuación, se detallan los indicadores a nivel del propósito:

Tabla 30 Indicadores de Resultado

Indicador	Meta Propósito
Actualizar la infraestructura tecnológica del Ministerio de Economía y Finanzas necesaria para la prestación eficiente de los servicios al sector público no Financiero.	100%

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo gestión del proyecto

4.3 Marco Lógico

Para evidenciar la programación del proyecto a continuación, se detalla el marco Lógico:

Tabla 31 Matriz de Marco Lógico

Resumen Narrativo de Objetivos	Indicadores verificables objetivamente	Medios de verificación	Supuestos
Fin			
Mantener la disponibilidad y continuidad de las aplicaciones y servicios tecnológicos del Sistema Nacional de las Finanzas Públicas, SINFIP, para que las entidades Sector Público no Financiero transacciones en una plataforma tecnológica actualizada, segura y confiable, para que ejecuten las actividades relacionadas con el PGE	Al 2024 el MEF contará con el 80% de infraestructura tecnológica actualizada	Reporte de obsolescencia de la infraestructura tecnológica del MEF	Los usuarios operan con confiabilidad disponibilidad, y seguridad los módulos de los sistemas informáticos
Propósito			
Actualizar la infraestructura tecnológica del Ministerio de Economía y Finanzas necesaria para la prestación eficiente de los servicios al sector público no Financiero.	Al 2024 el MEF contará con la actualización del el 100% de la infraestructura tecnológica obsoleta	Informe de Infraestructura Instalada del MEF	Se cuenta con el apoyo de las máximas autoridades, financiamiento y documentos habilitantes de Entes Rectores en los plazos programados.
Componentes			
1. Fortalecimiento la infraestructura tecnológica del SINFIP (Hardware)	Al 2024 el MEF contará con 4 equipos balanceadores de enlaces, DNS y aplicaciones, operativo	Informes técnicos de la instalación de la plataforma tecnológica	Se cuenta con los recursos financieros, talento humano, documentos habilitantes, disponibilidad de equipamiento requerido, proveedores calificados y buen ambiente de comercio a nivel nacional e internacional.

	Al 2024 el MEF contará con 5 equipos de seguridad firewall perimetral y firewall IPS, operativo	Informes técnicos de la instalación de la plataforma tecnológica	Se cuenta con los recursos financieros, talento humano, documentos habilitantes, disponibilidad de equipamiento requerido, proveedores calificados y buen ambiente de comercio a nivel nacional e internacional.
	Al 2024 el MEF contará con 5 equipos de infraestructura para el reforzamiento de conectividad LAN, operativo	Informes técnicos de la instalación de la plataforma tecnológica	Se cuenta con los recursos financieros, talento humano, documentos habilitantes, disponibilidad de equipamiento requerido, proveedores calificados y buen ambiente de comercio a nivel nacional e internacional.
	Al 2024 el MEF contará con 12 equipos de infraestructura y servicio para el reforzamiento de la nube privada, operativa	Informes técnicos de la instalación de la plataforma tecnológica	Se cuenta con los recursos financieros, talento humano, documentos habilitantes, disponibilidad de equipamiento requerido, proveedores calificados y buen ambiente de comercio a nivel nacional e internacional.
	Al 2024 el MEF contará con 7 equipos de para la gestión de respaldos operativos y 1 software actualizado	Informes técnicos de la instalación de la plataforma tecnológica	Se cuenta con los recursos financieros, talento humano, documentos habilitantes, disponibilidad de equipamiento requerido, proveedores calificados y buen ambiente de comercio a nivel nacional e internacional.
2. Reducción la brecha tecnológica y operativa del MEF (Software)	Al 2024 el MEF contará con 1 actualización de la versión de la Nube Privada operativa	Informe técnico de actualización de la nube privada	Se cuenta con los recursos financieros, talento humano, documentos habilitantes, disponibilidad de equipamiento requerido, proveedores calificados y buen ambiente de comercio a nivel nacional e internacional.
Actividades	**Monto con IVA**	**Medios de verificación**	**Supuestos**
1.1 Adquisición de equipos balanceadores de enlaces, DNS y aplicaciones para el Centro de Datos Principal del Ministerio de Economía y Finanzas	1.103.299,59	Contrato firmado, acta entrega recepción final	Se cuenta con el apoyo de las máximas autoridades, se cuenta con los recursos financieros, talento humano, documentos habilitantes, disponibilidad de equipamiento requerido, proveedores calificados y buen ambiente de comercio a nivel nacional e internacional.
1.2 Adquisición de equipos de seguridad firewall perimetral y firewall IPS de Data Center para el Centro de Datos Principal	1.026.308,64	Contrato firmado, acta entrega recepción final	Se cuenta con el apoyo de las máximas autoridades, se cuenta con los recursos financieros, talento humano, documentos habilitantes, disponibilidad de equipamiento requerido, proveedores calificados y

			buen ambiente de comercio a nivel nacional e internacional.
1.3 Adquisición de Infraestructura para el reforzamiento de conectividad LAN del Centro de Datos Principal del Ministerio de Economía y Finanzas	690.089,04	Contrato firmado, acta entrega recepción final	Se cuenta con el apoyo de las máximas autoridades, se cuenta con los recursos financieros, talento humano, documentos habilitantes, disponibilidad de equipamiento requerido, proveedores calificados y buen ambiente de comercio a nivel nacional e internacional.
1.4 Adquisición de Infraestructura y Servicio para el reforzamiento de la nube privada del Ministerio de Economía y Finanzas	1.745.310,43	Contrato firmado, acta entrega recepción final	Se cuenta con el apoyo de las máximas autoridades, se cuenta con los recursos financieros, talento humano, documentos habilitantes, disponibilidad de equipamiento requerido, proveedores calificados y buen ambiente de comercio a nivel nacional e internacional.
1.5 Adquisición de una solución integral de gestión de respaldos para el Ministerio de Economía y Finanzas	2.051.932,14	Contrato firmado, acta entrega recepción final	Se cuenta con el apoyo de las máximas autoridades, se cuenta con los recursos financieros, talento humano, documentos habilitantes, disponibilidad de equipamiento requerido, proveedores calificados y buen ambiente de comercio a nivel nacional e internacional.
2.1 Consultoría e implementación de la actualización de la versión de la Nube Privada	67.200,00	Contrato firmado, acta entrega recepción final	Se cuenta con el apoyo de las máximas autoridades, se cuenta con los recursos financieros, talento humano, documentos habilitantes, disponibilidad de equipamiento requerido, proveedores calificados y buen ambiente de comercio a nivel nacional e internacional.

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo gestión del proyecto

4.3.1 Anualización de las metas de los indicadores del propósito

A continuación, se detalla las metas de los indicadores de resultados asociados al proyecto:

Tabla 32 Metas de indicadores de propósito

Propósito: Actualizar la infraestructura tecnológica del Ministerio de Economía y Finanzas necesaria para la prestación eficiente de los servicios al sector público no Financiero.						
Indicador	**Unidad de Medida**	**Meta Propósito**	**Ponderación**	**2023**	**2024**	**Total**
Al 2024 contar con la actualización de la infraestructura tecnológica obsoleta	Porcentaje	100%	100%	0,00%	100,00%	**100%**
	Meta anual ponderada			0,00%	100,00%	**100%**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo gestión del proyecto

5. ANÁLISIS INTEGRAL

5.1 Viabilidad Técnica

5.1.1 Descripción de la Ingeniería de Proyecto

El proyecto responde a la necesidad de actualizar la plataforma tecnológica del Ministerio de Economía y Finanzas, cuyo estado de obsolescencia implica un gran riesgo para la prestación de los servicios que se entregan a las entidades a través del sistema de gestión de las finanzas públicas; a continuación, se explica la funcionalidad de **los equipos que se adquirirán para cumplir el objetivo del proyecto**:

Equipos balanceadores, en la arquitectura de las aplicaciones del Sistema de las Finanzas Públicas, tienen la función de balancear las peticiones de los usuarios a los diferentes aplicativos o sistemas, que a su vez van hacia los diferentes equipos *servidores de aplicación* que se encuentran en granjas[2]; otra funcionalidad destacada de estos equipos es la de balancear los enlaces de comunicación junto con las peticiones de DNS[3].

El equipamiento y la fecha de fin de vida útil:

- F5 BIG-IP 8900-R *Fueron soportadas hasta 1 de febrero 2022*
- F5 BIG-IP 3600-4GR *Fueron soportadas hasta 1 de octubre 2021*

[2] Una granja de servidores es un grupo de servidores que se mantienen en una única localización. Todos estos servidores están conectados de forma conjunta, haciendo que puedan realizar cosas que pueden resultar difíciles o imposibles de hacer por un solo servidor. Con una granja de servidores, toda la carga de trabajo es distribuida entre múltiples componentes en los servidores, lo cual provee de una gran capacidad para realizar procesos informatizados. (¿Qué es una Granja de Servidores? (ordenadores-y-portatiles.com)

[3] El **sistema de nombres de dominio** (*Domain Name System* o **DNS**, por sus siglas en inglés)[1] es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombres de dominio asignados a cada uno de los participantes. Su función más importante es «traducir» nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente. (Sistema de nombres de dominio - Wikipedia, la enciclopedia libre

Equipos firewall o cortafuegos, son equipos utilizados para la seguridad de la red y todas sus comunicaciones, funcionan como un sistema diseñado para proteger el acceso no autorizado y no verificado en una conexión desde el internet o internamente a las aplicaciones, bloqueando los accesos a las redes internas donde se encuentran los equipos servidores que soportan a las aplicaciones del Sistema de las Finanzas Públicas, a continuación, su descripción y fecha de fin de vida útil:

- ASA5540-AIP20-K *Fueron soportadas hasta 16 de septiembre 2013*
- ASA5580-20-BUN-K8 *Fueron soportadas hasta 31 de julio 2012*

El Switch de core o conmutador es un equipo de interconexión, que se utiliza para conectar equipos en red, formando lo que se conoce como una red de área local, estos equipos se encargan del enrutamiento y conmutación del tráfico de los equipos en la red.

- WC-C6509-E *Fueron soportadas hasta 30 de octubre 2020*
- VS-C6509E-S720-10G *Fueron soportadas hasta 31 de julio 2015*

Equipamiento de la Nube Privada, la nube privada es un conjunto de equipos físicos que utilizan una tecnología de virtualización para combinar recursos en una organización o entidad; su principal característica es la flexibilidad en la asignación de recursos, escalabilidad y la optimización de uso de los recursos tecnológicos. El fabricante de los equipos de la Nube Privada del Ministerio de Economía y Finanzas, el fabricante de los equipos ha declarado el fin de soporte (End of Support Life EOSL) para el 31 de agosto de 2023 para los elementos de comunicación Virtual Connect SAN de los chasis de la Nube Privada, posterior a esta fecha no existe posibilidad de ningún servicio de renovación.

Plataforma de respaldos, es el equipamiento y el software que trabajan de una manera coordinada, en un proceso que permite guardar información crítica e importante de los sistemas, en uno o más dispositivos de almacenamiento, existen varios medios de almacenamiento como son: cintas de respaldo, almacenamiento de corta o larga retención, entre otros. El fabricante de estos equipos comunica que el fin de soporte (End of Support Life EOSL) de estos equipos es el 31 de diciembre de 2022 para la Librería Virtual VLS (EVA 440) y Librería Física (ESL 322e), posterior a esta fecha no existe posibilidad de ningún servicio de renovación.

5.1.1.1 Componentes del proyecto

En el marco de los objetivos del proyecto, analizando las causas del problema planteado y lo requerido para solventarlo y cumplir el objetivo se definen como resultado del árbol de objetivos dos componentes:

Componente 1: Fortalecimiento la infraestructura tecnológica del SINFIP (Hardware)

Este componente satisface la necesidad tecnológica de poseer una plataforma actualizada, que está cubierta por garantía y soporte de fábrica, y reemplace el equipamiento obsoleto o el que está finalizada su vida útil. Tal como se ha indicado en los párrafos anteriores, existe 5 grupos de infraestructura que requieren ser reemplazados:

- Equipos balanceadores
- Equipos de seguridad o firewalls
- Equipo de comunicación o switch
- Equipamiento para la Nube Privada
- Sistema de respaldos

Cada uno tiene su ámbito de acción y cobertura tecnológica dentro de la operación de los sistemas de gestión financiera que atienden a las diferentes entidades. La necesidad para lograr el objetivo se plasma en 5 contratación que cubran este equipamiento, a continuación, el resumen del alcance de cada una de ellas:

Actividad 1.1 Adquisición de equipos balanceadores de enlaces, DNS y aplicaciones para el centro de datos principal del Ministerio de Economía y Finanzas.

El objetivo de esta contratación es reemplazar los equipos balanceadores con características de: DNS y protección contra ataques de denegación de servicio; equipos para balanceo de aplicaciones para el Centro de Datos Principal manteniendo las configuraciones actuales de las aplicaciones del SINFIP.

El alcance de esta contratación es el de contar con una infraestructura de equipos balanceadores con características de: DNS y protección contra ataques de denegación de servicio; y equipos para balanceo y seguridad, con la capacidad necesaria y suficiente para soportar las aplicaciones del SINFIP, compatible con su arquitectura y garantizando la disponibilidad, el rendimiento y seguridad de todos los ambientes productivos y no productivos en el Centro de Datos Principal. Fortaleciendo la seguridad de los aplicativos SINFIP con soluciones de última generación, garantizando similar funcionalidad y la continuidad de las aplicaciones. Incluye además el soporte y garantía vigentes con fabricantes.

Actividad 1.2 Adquisición de equipos de seguridad firewall perimetral y firewall IPS de data center para el Centro de Datos Principal

El objetivo de esta contratación es reemplazar los equipos de seguridad de data center y perimetral para el Centro de Datos Principal manteniendo las configuraciones actuales de las aplicaciones del SINFIP.

El alcance es contar con una infraestructura de equipos de seguridad firewall perimetral y firewall IPS de Data center con la capacidad necesaria y suficiente para soportar las aplicaciones del SINFIP, compatible con su arquitectura y garantizando la disponibilidad, el rendimiento y seguridad de todos los ambientes productivos y no productivos en el Centro de Datos Principal. Fortalecer la seguridad de los aplicativos SINFIP con soluciones de última generación, garantizando similar funcionalidad y la continuidad de las aplicaciones. Disponer de soporte y garantía vigentes con fabricantes.

Actividad 1.3 Adquisición de infraestructura para el reforzamiento de conectividad LAN del Centro de Datos principal del Ministerio de Economía y Finanzas

El objetivo de esta contratación es adquirir una infraestructura de red de conectividad LAN que disponga de alta disponibilidad con vigencia tecnológica, capacidad de crecimiento y que soporte las necesidades actuales y futuras para el Centro de Datos del Ministerio de Economía y Finanzas en la ciudad de Quito.

El alcance es actualizar la infraestructura de conectividad en capa 2 y 3 del Centro de Datos Principal de esta Cartera de Estado, a una capacidad adecuada para el correcto funcionamiento de los aplicativos de los Sistemas de las Finanzas Públicas; implementando una arquitectura de alta disponibilidad en la red Core LAN del Centro de Datos Principal, con la adquisición de un switch de core secundario con arquitectura compatible con el switch de core LAN actual.

Con esto se soportará los requerimientos de disponibilidad, continuidad de las aplicaciones y herramientas del SINFIP y de esta manera proporcionar un servicio adecuado a las instituciones que acceden a dichas aplicaciones. Disponer de soporte y garantía vigentes con fabricantes.

Actividad 1.4 Adquisición de infraestructura y servicio para el reforzamiento de la nube privada del Ministerio de Economía y Finanzas

El objetivo de esta contratación es contar con infraestructura con vigencia tecnológica y capacidad de crecimiento para poder soportar las necesidades que los ambientes productivos y no productivos del Sistema Nacional de las Finanzas Públicas SINFIP requieren para su normal operación.

Su alcance es tener una infraestructura con vigencia tecnológica de más de cinco años, con soporte y garantía directo del fabricante; con una capacidad de crecimiento para cumplir los requerimientos de memoria y procesador que las aplicaciones y servicios del SINFIP necesitan, con lo que se tendrá la posibilidad de creación de nuevos servidores de aplicación de acuerdo a las necesidades existentes y futuras, permitirá además la redistribuir los recursos de memoria y procesador entre los servidores; y finalmente teniendo la capacidad para la migración a la última versión de su hipervisor.

Actividad 1.5 Adquisición de una solución integral de gestión de respaldos para el Ministerio de Economía y Finanzas

El objetivo de esta contratación es contar con una solución para la gestión, administración de los procesos de respaldo de la información, que permitirá garantizar la disponibilidad de la misma y su recuperación ante cualquier incidente de perdida de información que pudiera presentarse. Adquiriendo una nueva solución que permita, para contar con solución de gestión de respaldos con vigencia tecnológica con soporte del fabricante, con capacidad de crecimiento para cumplir los requerimientos de almacenamiento de nuevos respaldos de acuerdo a las necesidades de negocio, implementando nuevas tecnologías de seguridad en los respaldos para la prevención de ataques del tipo Ransomware, garantizando la validez y confiabilidad de los respaldos; y finalmente contando con almacenamiento suficiente en la solución de respaldos a fin de mantener la información por el tiempo que lo determina la ley.

Componente 2: Reducción la brecha tecnológica y operativa del MEF (Software)

Este componente satisface la necesidad de reducir la brecha tecnológica y operativa del Ente Rector en cuanto a las versiones de software se refieren, permitiendo la contratación de especialistas con alto nivel de experiencia y conocimiento para migrar versiones de software base sobre el que corren los sistemas y aplicativos del sistema de las finanzas públicas, este componente abarca servicios especializados y no compra de licencias o software adicional.

Actividad 2.1 Consultoría para la actualización de la Nube Privada

El objetivo de esta consultoría es contratar especialistas de alto conocimiento en Nube Privada y en hipervisor Hyper V, que es el que se utiliza en el Ente Rector y es el responsable de la gestión y virtualización de servidores, que conforman la Nube Privada.

El alcance es Actualizar la versión del software base de la Nube Privada de Producción a Windows Server Data Center 2019. El licenciamiento de estas nuevas versiones no son parte de esta contratación, ya que el Ministerio de Economía y Finanzas posee el derecho de actualización de la versión actual hacia la del objetivo planteado.

5.1.2 Especificaciones técnicas

A continuación, se describen las especificaciones técnicas de los equipos requeridos para cumplir con los objetivos del proyecto, y proporcionar sostenibilidad tecnológica en los siguientes 5 años, de acuerdo al componente y actividad.

Componente 1: Fortalecimiento la infraestructura tecnológica del SINFIP (Hardware)

Actividad 1.1 Adquisición de los equipos balanceadores de enlaces, DNS y aplicaciones para el centro de datos principal del Ministerio de Economía y Finanzas.

La presente contratación busca el reemplazo de los equipos balanceadores y de seguridad, mediante la implementación de equipos con vigencia tecnológica y que sean compatibles con las configuraciones actuales que se requieren para que las aplicaciones no tengan afectación en su funcionamiento.

Las actividades de reemplazo de los equipos balanceadores deben realizarse con el mínimo impacto y manteniendo la operatividad de las Aplicaciones del SINFIP.

Para lo cual se requiere:

- Adquirir 2 equipos balanceadores de enlaces y DNS, y protección contra ataques de denegación de servicio en alta disponibilidad con las siguientes características:

Tabla 33 Especificaciones técnicas Equipos Balanceadores de enlaces y DNS

Especificación	Requerimiento Mandatorio
Cantidad	2 (dos).
Marca	Indicar.
Modelo	Indicar. El equipo ofertado debe ser el último modelo liberado para la venta por el fabricante y que cumpla con las especificaciones técnicas indicadas.
Año de fabricación	>=2022
Procedencia	Nuevo de fábrica. No se aceptarán equipos re manufacturados.
Tipo	El equipo ofertado debe ser una plataforma de hardware de propósito específico denominado Appliance dedicados para balanceo de enlaces y DNS, y mitigación de ataques DDoS.

Características Físicas y de Rendimiento	El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir, un sistema operativo desarrollado por el fabricante específicamente para propósitos de Balanceo de Carga de Servicios y Seguridad de Aplicaciones basadas en protocolo IP (TCP/UDP) y servicios web
	Los valores de desempeño solicitados deberán ser logrados por el equipo “appliance” como un sistema independiente y autónomo que cumpla el desempeño exigido y no como la suma o agregación de varios "appliance" que logren sumar el valor solicitado
	Cada equipo de los dos ofertados, debe cumplir con las siguientes características:
	La solución debe soportar un Throughput en L7/L4 >= 55 Gbps
	La solución debe soportar >= 40 Millones de conexiones simultáneas
	La solución debe soportar >= 800.000 conexiones por segundo en L4
	Cada equipo de los ofertados, debe contar con al menos las siguientes Interfaces de red:
	>= 8 puertos SFP+, con opción de conectividad de 10 Gbps de fibra
	>= 2 puertos QSFP+ de 40 Gbps.
	>= 1 puerto de administración de 1 Gbps.
	Incluir 5 transceivers de 10 Gbps de fibra
	Incluir sus respectivos patchords de fibra
	Para mejorar el rendimiento de la sincronización de configuración deberá poder sincronizar la configuración de manera incremental
	Ante la necesidad de conmutar el tráfico a otros dispositivos del grupo, el sistema deberá poder realizar cálculos para determinar el mejor dispositivo basado en: recursos, capacidad, carga de tráfico en cada dispositivo. Identificando la mejor opción cuando el ambiente sea heterogéneo en cuanto se refiere a plataformas.
	La configuración será sincronizada entre todos los dispositivos del grupo pudiendo escoger si la sincronización se realiza de manera automática o manual.
	Los equipos deben contar con aceleración, con la capacidad de manejar perfiles de acuerdo a las funciones que vaya a ejecutar, como, por ejemplo: protección DDoS, protocolos SDN y manejo de trafico de L4, TCP, UDP, IPv6

Alta Disponibilidad	Los equipos deben tener la característica de soportar alta disponibilidad, es decir, tener la capacidad de conectarse a una unidad similar y operar en modo activo y la otra unidad en modo pasivo (fail-over) y deberá contar con la capacidad de direccionamiento virtual. Cada equipo debe tener la capacidad de recuperar las sesiones del sistema en forma inmediata y automática en caso de fallo de: un adaptador, cable de red, canal de controladora o alimentación de fluido eléctrico.
	Se debe ofertar 2 (dos) equipos en Alta disponibilidad funcionando en configuración activo - pasivo. Por razones de eficiencia de uso de la energía, la climatización, uso de espacio en rack, administración y facilidad de configuración, no se aceptará soluciones basadas en cluster virtual de múltiples equipos
Instalación	Los equipos deberán ser instalados en un rack estándar de 19” de propiedad del Ministerio de Economía y Finanzas.
Redundancia en fuente de poder	Cada equipo debe contar con fuentes de poder redundantes AC, entradas de voltaje de 110 a 220 VAC que se puedan remover en caliente (hot-swap).
Funciones de DNS y Balanceo Global	El sistema debe incluir licenciamiento para solución de gestión, resolución y seguridad de DNS, debe ser de la misma marca de toda la solución ofertada. No se aceptan soluciones standalone ni de fabricantes diferentes.
	La licencia de balanceo global deberá funcionar sobre una instancia virtual diferente e independiente, en los mismos equipos ofertados. Los recursos físicos para esta funcionalidad deben ser dedicados sin compartición con la funcionalidad de protección contra DDoS.
	Debe funcionar como un servidor DNS autoritativo de alto desempeño, permitiendo manejar un dominio completo o delegación de parte de un dominio. Debe ser DNS cache autónomo sin necesidad de balancear requerimientos DNS a una granja de servidores DNS.
	Para el balanceo global (DNS), debe permitir al menos los siguientes métodos de balanceo estático y dinámico, de manera nativa y no a través de configuración por scripting:
	Round Robin
	Least Connections
	Packets Per Second
	Round Trip Time
	Persistencia estática
	Debe manejar persistencia a nivel global, manteniendo a los usuarios en un mismo datacenter por el transcurso de su sesión.
	Permitir Balanceo de cargas ente datacenters de acuerdo a la ubicación geográfica.

Debe permitir la creación de topologías personalizadas con el fin de permitir distribución de tráfico basado en requerimientos particulares de la infraestructura
Debe permitir monitoreo de la infraestructura y las aplicaciones a balancear, integrándose con otros equipos del mismo fabricante o de terceros.
Debe soportar el protocolo DNSSEC
Debe incluir herramienta de administración grafica para el manejo de zonas DNS
Debe soportar registros AAAA para IPv6
Debe soportar traducción entre DNS IPv4 y DNS IPv6
La solución debe soportar >=1 Millones de respuestas DNS por segundo.
La solución debe tener la capacidad de almacenar respuestas DNS en cache
La solución debe proteger contra ataques de denegación de servicio al DNS tales como UDP fllood, DNS query flood, NXDOMAIN floods y paquetes mal formados.
La solución debe incluir funcionalidades de firewall DNS tales como:
- ACL según tipo de DNS record
- Bloqueo de respuestas no solicitadas
- IP Anycast
- Configurar límites de respuestas DNSSEC
- Configuración y alertas basados en límites de conexiones configurados.
- Configuración de umbrales de números de conexiones
- Reportes y logs DNS
La solución ofertada debe tener la capacidad de responder las peticiones DNS con la dirección IP pública del mejor Centro de Datos disponible, todo basado en:
- Geolocalización
- Desempeño del Centro de datos
- Balanceo entre ambientes híbridos
La solución ofertada debe proveer estadísticas detalladas basadas en el tipo de consulta: A, CNAME, NS, AAAA, SRV entre otras. Debe mostrar estadísticas de respuestas por perfil y por dispositivo.
La solución debe soportar el permitir alta disponibilidad y agregación de tráfico para dos o más enlaces de Internet.
Debe manejar persistencia a nivel global, manteniendo a los usuarios en un mismo canal por el transcurso de su sesión

	No debe tener un límite por licenciamiento o funcional para el número de enlaces que se pueden balancear.
Funciones de Protección DDoS	El sistema debe incluir licenciamiento para protección y mitigación de ataques de denegación de servicio DDoS, sobre los mismos equipos ofertados, debe ser de la misma marca de toda la solución ofertada. No se aceptan soluciones standalone ni de marcas diferentes. La solución contra DDoS deberá trabajar en una instancia virtual independiente de modo que los recursos de hardware sean dedicados para esta parte del equipo. No se deberán compartir recursos de hardware entre las funcionalidades de balanceo global y anti DDoS.
	Debe incluir protección contra ataques de DDoS en capas 4-7 utilizando vectores de ataque personalizables
	Debe bloquear ataques a nivel de red como flood, sweep, teardrop, smurf attacks
	Debe mitigar ataques basados en protocolos, incluyendo SYN, ICMP, ACK, UDP, TCP, IP, DNS, ICMP, ARP
	Debe permitir la creación de reglas basadas en aplicación, independientes para cada una de ellas.
	Debe permitir la creación de reglas globales.
	Debe permitir la creación de reglas de protección contra DDoS
	Debe tener la opción de funcionar como un firewall statefull full-proxy
	Debe permitir la creación de listas blancas (White lists) de direcciones IP
	Debe brindar protección contra Ataques de Denegación de Servicio para el protocolo DNS, poder controlar el tráfico DNS de acuerdo al tipo de Registro solicitado y detectar anomalías a nivel del protocolo
	Debe permitir personalizar los Logs, y ser exportados a un repositorio Syslog externo.
	Debe funcionar como un Proxy SSH para control de conexiones entre diferentes redes con el fin de dar visibilidad a las sesiones SSH y controlar las mismas
	Debe soportar e incluir Geolocalización de direcciones IP
	Debe permitir la personalización de la protección contra ataques de denegación de servicio utilizando umbrales modificables por el administrador.
Estándares de Red	Soporte VLAN 802.1q, Vlan tagging
	Soporte de 802.3ad para definición de múltiples troncales
	Soporte de NAT, SNAT
	Soporte de IPv6: El equipo debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente.
	Soporte de Rate Shapping.

	Soporte de dominios de Enrutamiento, donde cada uno pueda tener su propio Default Gateway y estar conectados a redes IP con el mismo direccionamiento.
	Debe soportar protocolos de enrutamiento BGP, RIP, OSPF, IS-IS
Administración del Sistema	La solución debe permitir el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH, interfaz de administración gráfica basada en Web seguro (HTTPS)
	La solución debe integrarse con LDAP, para la autenticación de usuarios para gestión de la herramienta.
	La solución debe integrarse con RADIUS y TACACS+ para la autenticación de usuarios para gestión de la herramienta.
	La solución debe incluir comunicación cifrada y permitir la autenticación del equipo y de los usuarios administradores/supervisores con Certificados Digitales
	La solución debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante:
	· Protocolo SysLog
	· Notificación vía SMTP
	· SNMP versión.2.0 o superior.
	El sistema de administración debe ser totalmente independiente del sistema de procesamiento de tráfico.
	El equipo debe contar con un módulo de administración tipo lights out que permita encender/apagar el sistema de manera remota y visualizar el proceso de arranque.
	La interfaz gráfica debe contar con un Dashboard personalizable que permita monitorear el estado del equipo en tiempo real
	Debe contar con un módulo de reportes que permita visualizar gráficamente el comportamiento de las aplicaciones HTTP como latencias hacia los servidores, latencias en los URL, Direcciones IPs que acceden las aplicaciones, URLs más visitados en las aplicaciones, Throughput hacia los servidores y estadísticas acerca de los servicios creados y los servidores físicos.
	Debe Contar con plantillas para la implementación rápida de aplicaciones de mercado conocidas (ej, Oracle, Microsoft, SAP, IBM) y permitir crear plantillas personalizadas que puedan ser actualizadas/exportadas entre equipos.
Virtualización	Cada uno de los equipos ofertados deben tener la capacidad de correr al menos 4 instancias virtuales independientes en el mismo hardware
	Cada una de las instancias virtuales debe comportarse como un dispositivo independiente, debe tener asignado capacidades específicas de CPU, memoria y almacenamiento.

	Cada una de las instancias virtuales debe permitir realizar su propia configuración, la cual debe poder ser totalmente diferente a las demás instancias.
	Cada instancia virtual debe tener sus propios logs
	El hypervisor sobre el cual corren las diferentes instancias virtuales debe ser del mismo fabricante y diseñado con este propósito específico para alojar solo el software del fabricante.
	Las instancias virtuales deben tener la capacidad de correr diferentes versiones del sistema operativo. Es decir, no necesariamente todas las instancias virtuales deben correr la misma versión de sistema operativo.
	Una de las instancias virtuales deberá utilizarse para realizar pruebas de nuevo firmware y en general pruebas de nuevas configuraciones. Esto no debe afectar a las demás instancias virtuales de producción.
	Las instancias virtuales deben permitir reiniciarse individualmente, sin que esto afecte a las demás instancias virtuales
	La asignación de recursos a cada instancia debe poder ser modificada, sin que esto afecte la normal operación de dicha instancia virtual y sin la necesidad de reiniciar la misma

- Adquirir 2 equipos para balanceo y seguridad de aplicaciones en alta disponibilidad con las siguientes características:

Tabla 34 Especificaciones técnicas Equipos balanceo y seguridad de aplicaciones

Especificación	Requerimiento Mandatorio
Cantidad	2 (dos).
Marca	Indicar.
Modelo	Indicar. El equipo ofertado debe ser el último modelo liberado para la venta por el fabricante y que cumpla con las especificaciones técnicas indicadas.
Año de fabricación	>=2022
Procedencia	Nuevo de fábrica. No se aceptarán equipos re manufacturados.
Tipo	Los equipos ofertados deben ser una plataforma de hardware de propósito específico denominado Appliances dedicados para balanceo y seguridad de aplicaciones

	El sistema operativo de los equipos ofertados debe ser de propósito específico y no uno de uso genérico, es decir, un sistema operativo desarrollado por el fabricante específicamente para propósitos de Balanceo de Carga de Servicios y Seguridad de Aplicaciones basadas en protocolo IP (TCP/UDP) y servicios web
	Los valores de desempeño solicitados deberán ser logrados por el equipo "appliance" como un sistema independiente y autónomo que cumpla el desempeño exigido y no como la suma o agregación de varios "appliance" que logren sumar el valor solicitado
	Cada equipo debe cumplir con las siguientes características:
	· Throughput en L7/L4 >=60 Gbps
	· Soportar >= 60 Millones de conexiones simultáneas.
	· Soportar >= 800.000 de conexiones por segundo en L4.
	Cada equipo debe contar con al menos las siguientes Interfaces de red:
Características Físicas y de Rendimiento	· >= 8 puertos SFP+ con opción de conectividad 10 Gbps
	· >= 2 puertos QSFP+ de 40 Gbps.
	· >= 1 puerto de administración de 1 Gbps.
	· Incluir 5 transceivers de 10 Gbps de fibra
	· Incluir sus respectivos patch cords de fibra.
	Cada equipo debe contar con fuentes de poder redundantes AC, entradas de voltaje de 110 a 220 VAC que se puedan remover en caliente (hot-swap).
	Para mejorar el rendimiento de la sincronización de configuración el equipo deberá poder sincronizar la configuración de manera incremental
	Ante la necesidad de conmutar el tráfico a otros dispositivos del grupo, el sistema deberá poder realizar cálculos para determinar el mejor dispositivo basado en: recursos, capacidad, carga de tráfico en cada dispositivo. Identificando la mejor opción cuando el ambiente sea heterogéneo en cuanto se refiere a plataformas.
	La configuración será sincronizada entre todos los dispositivos del grupo pudiendo escoger si la sincronización se realiza de manera automática o manual.
Alta Disponibilidad	

	Los equipos deben tener la característica de soportar alta disponibilidad, es decir, tener la capacidad de conectarse a una unidad similar y operar en modo activo y la otra unidad en modo pasivo (fail-over) y deberá contar con la capacidad de direccionamiento virtual. Cada equipo debe tener la capacidad de recuperar las sesiones del sistema en forma inmediata y automática en caso de fallo de: un adaptador, cable de red, canal de controladora o alimentación de fluido eléctrico.
	Se debe ofertar 2 (dos) equipos en Alta disponibilidad funcionando en configuración activo - pasivo. Por razones de eficiencia de uso de la energía, la climatización, uso de espacio en rack, administración y facilidad de configuración, no se aceptará soluciones basadas en cluster virtual de múltiples equipos
Instalación	Los equipos deberán ser instalados en un rack estándar de 19”.
Administración de Tráfico	Los equipos deben realizar funciones de balanceo de tráfico a aplicaciones basadas en TCP/UDP, incluidos servicios web.
	La solución debe permitir la definición de dirección IP y puerto virtual para la prestación de un servicio. El puerto del servicio puede ser distinto al puerto que usan los servidores.
	La solución debe tener arquitectura Full-Proxy, control de entrada y salida de conexiones distinguiendo conexiones del lado del cliente y del lado del servidor o los recursos.
	La solución ofertada debe ser capaz de soportar balanceo amortiguado de los nuevos servidores que sean agregados, para prevenir la saturación de conexiones. De manera que servidores que se agregan al grupo de balanceo, reciban al inicio menos cantidad de peticiones por un tiempo determinado, hasta ser capaz de recibir la misma cantidad de peticiones que los que ya estaban en el grupo.
	Los equipos ofertados deberán permitir hacer persistencia de conexiones hacia la aplicación con base en cualquier información contenida en cualquier parte del paquete completo, esto para poder adaptar la solución a las necesidades de las diferentes aplicaciones
	La solución debe permitir hacer control de balanceo de tráfico según se defina entre uno o varios tipos de algoritmos especializados de balanceo. Estos métodos deben realizarse de manera nativa y no por medio de configuración por scripting:
	· Round Robin
	· Proporcional (Ratio)
	· Respuesta más rápida
	· Menor número de sesiones

El equipo ofertado debe no tener restricciones en el número de servicios virtuales que se pueden configurar (Virtual Servers, Virtual IP, granjas)
El sistema debe ser capaz de identificar fallos en servicios para redundancia de las aplicaciones.
La solución debe realizar monitoreo de la salud de los Servidores que gestione el equipo de Balanceo de tráfico, por medio de:
· Ping.
· Chequeo a nivel de TCP y UDP a puertos específicos
· Monitoreo http y https
· Verificación de la salud de una combinación de servicios, permitiendo tomar la decisión del estado de salud aplicando varios monitores simultáneos.
· Configurar monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red.
· Monitoreos en línea, donde el funcionamiento de la aplicación determine el estado de salud de la misma
· Monitoreo de aplicaciones de mercado:
o LDAP
o FTP
o SMTP
o IMAP/POP3
o Oracle
o MSSQL
o MySQL
o RADIUS
o SIP
o Protocolo SASP
o SOAP
o SNMP
La solución debe permitir realizar todos estos métodos de persistencia de las conexiones:
· Dirección IP origen
· Dirección IP destino
· Cookies
· Hash
· SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia
· Sesiones SSL
· Microsoft Remote Desktop

	La solución ofertada debe soportar los 3 métodos de persistencia por Cookie: Cookie Insert, Cookie Pasivo y Cookie Rewrite.
	La solución debe garantizar afinidad del servidor, de tal forma que una solicitud de un cliente y cada solicitud posterior se dirijan al mismo servidor de la granja.
	La solución ofertada Deberá permitir modificar el contenido HTML utilizando objetos de configuración y sin necesidad de generar scripts.
	Los equipos deben ser compatibles con tráfico IPSEC
	La solución Debe soportar e incluir Geolocalización, de manera que pueda tomar decisiones basado en una base de datos de continentes, países y de direcciones IP.
	La Base de datos de geolocalización debe incluir los países de América Latina y estar disponible en el mismo equipo sin necesidad de acceso a Internet (offline).
Funciones de Seguridad	Cada equipo debe soportar seguridad SSL con las siguientes características:
	· Incluir el soporte de Aceleración SSL usando Hardware Dedicado
	· Incluir mínimo 25.000 Transacciones por segundo SSL (RSA 2K Keys)
	· Incluir mínimo 28.000 Transacciones por segundo SSL (ECDSA P-256)
	· Soportar al menos 30 Gbps SSL Bulk Encryption (Thoughput SSL)
	· Soporte de llaves SSL RSA de 1024, 2048 y 4096 bits
	Debe soportar TLS 1.3, final o draft
	La solución debe soportar mirroring de sesiones SSL. Si el equipo primario falla el equipo secundario debe mantener la sesión SSL
	El Stack TLS del equipo debe soportar las siguientes funcionalidades/características
	· Session ID
	· Session Ticket
	La solución debe manejar AES, AES-GCM, SHA1/MD5 y soporte a algoritmos de llave pública: RSA, Diffie-Hellman, Digital Signature Algorithm (DSA) y Elliptic Curve Cryptography (ECC)
	Los equipos deben soportar firmado criptográfico de cookies para verificar su integridad.
	Los equipos deben tener la capacidad de integración con dispositivos HSM externos.

	La solución debe permitir la funcionalidad Proxy SSL, esta funcionalidad permite que sesión SSL se establezca directamente entre el usuario y el servidor final, sin embargo, el equipo balanceador debe ser capaz de desencriptar, optimizar y reencriptar el tráfico SSL sin que el balanceador termine la sesión SSL.
	La solución debe soportar HSTS (HTTP Strict Transport Security)
Funciones de Aceleración de Tráfico	La solución debe incluir la capacidad de hacer aceleración de aplicación a nivel de:
	· Memoria cache.
	· Compresión tráfico HTTP
	· Optimización de conexiones a la aplicación a nivel TCP
	· Multiplexación de conexiones hacia los servidores
	Cada equipo debe contar con una capacidad de compresión de tráfico a una tasa de 15 Gbps o superior usando aceleración por Hardware dedicado, no la CPU de propósito general.
	Cada equipo debe soportar el protocolo HTTP2.
Firewall de Aplicaciones WEB	La solución debe incluir funcionalidad de Firewall de Aplicaciones (WAF) en el mismo equipo, no debe ser un appliance independiente (para optimización de latencias, administración, espacio en rack, energía eléctrica, soportes de fabricante).
	La funcionalidad de WAF debe permitir la personalización de la política, de manera que se pueda ajustar finamente de acuerdo al servicio específico que estará protegiendo, sus URLs, parámetros, métodos, de manera específica.
	La solución debe trabajar en un esquema proxy TCP reverso y/o transparente
	La solución debe permitir la creación automática de políticas, deberá unificar múltiples URLs explicitas utilizando wildcards de manera de reducir la cantidad de objetos en la configuración.
	La solución debe trabajar en modo de bloqueo o en modo informativo
	La solución debe permitir diferentes políticas de seguridad para diferentes aplicaciones
	La solución debe permitir la creación de firmas personalizadas
	La solución debe trabajar con modelos de seguridad positiva y negativa (seguridad híbrida)
	La solución debe poder aprender el comportamiento de la aplicación automáticamente sin intervención humana
	La solución debe permitir personalizar las páginas de bloqueo incluyendo la capacidad de responder a webservices mediante un código HTTP 500.

El WAF debe permitir personalizar las páginas de bloqueo
La solución debe prevenir exponer el “OS fingerprinting”
La solución debe permitir la integración con Herramientas de verificación de vulnerabilidades, en particular WhiteHat, Cenzic, Qualys, IBM AppScan, HP WebInspect.
El WAF Debe soportar:
· Restringir protocolo y versión utilizada
· Validar URL-encoded characters
· Restringir la longitud del método de request
· Restringir la longitud del URI solicitado
· Restringir el número de Encabezados (headers)
· Restringir la longitud del nombre de los encabezados
· Restringir la longitud del valor de los encabezados
· Restringir la longitud del cuerpo (body) de la solicitud
· Restringir la longitud del nombre y el valor de las cookies
· Restringir el número de cookies
· Restringir la longitud del nombre y valor de los parámetros
· Restringir el número de parámetros
El WAF Debe incluir protección a Web Services XML y restringir el acceso a métodos definidos vía Web Services Description Language (WSDL)
El WAF debe incluir protección contra el Top 10 de ataques definidos en OWASP
El WAF debe incluir protección contra Web Scraping
La solución debe ser Session-aware es decir identificar y forzar que el usuario tenga una sesión e identificar los ataques por usuario
La solución debe permitir la definición y detección de las condiciones a cumplir para que una aplicación externa que vía Java realiza un requerimiento cross-domian, permitiendo evitar un CORS (Cross-Origin Resource Sharing).
Debe permitir verificar las firmas de ataque en las respuestas del servidor al usuario
Debe permitir el enmascaramiento de información sensible filtrada por el servidor
Debe poder bloquear basado en la ubicación geográfica e incluir la base de datos de geolocalización.
Debe permitir la integración con servidores Antivirus por medio del protocolo ICAP
Debe proteger contra ataque DoS /DDoS de Capa 7

Una vez detectado un ataque deberá ser posible descartar todos los paquetes que provengan de una dirección IP sospechosa
En caso de detectarse un ataque se requiere tener la posibilidad de iniciar una captura de tráfico (tipo tcpdump) para poseer información forense.
El WAF debe poder perfilar dinámicamente el tráfico y crear firmas de patrones de tráfico anómalos, deteniendo los ataques DoS de la capa 7 antes de que afecten a su aplicación, incluidos los ataques "Día Cero".
El WAF deberá poder encriptar dinámicamente el contenido de la página para evitar ataques de "man-in-the-browser" generalmente causados por malware, debera poder también cifra dinámicamente las credenciales a medida que se ingresan para proteger al usuario en el navegador.
El WAF debera contar con la posibilidad de mitigar ataques generados por BOTNETS o por Bots los cuales intentan suplantar el comportamiento de los usuarios, así mismo este debera proveer la detección y el bloqueo de amenazas automatizadas a nivel de sesión.
La solución debe ser capaz de diferenciar personas reales de Bots.
La solución debe poder desafiar a los posibles bots con un captcha
La solución debe soportar ofuscación de parámetros
La solución deberá tener la capacidad de proteger aplicaciones web que incluyan el contenido de servicios web (xml). La protección XML deberá contar con mecanismos automatizados de aprendizaje, similares a los de la protección de aplicaciones web.
El WAF Debe incluir protección a Web Services REST y XML y restringir el acceso a métodos definidos vía Web Services Description Language (WSDL) o OpenAPI v 3.0
La solución deberá:
- Inspeccionar y monitorear todos los datos http y la aplicación, incluyendo, los encabezados http, campos de formularios, y el cuerpo http.
- Inspeccionar las peticiones y respuestas http.
- Tener la habilidad de decodificar datos a su mínima expresión a partir de diferentes sistemas de encoding Web y validarla.
- Validar todos los tipos de datos ingresados, incluyendo URLs, formularios, cookies, cadenas de queries, campos y parámetros ocultos, métodos http, elementos XML y acciones SOAP.
La solución deberá permitir aplicar parches virtuales a aquellas vulnerabilidades detectadas por el sistema u obtenidas de terceros sobre el servidor de aplicación monitoreado

	Debe proteger como mínimo:
	· Ataques de Fuerza Bruta
	· Cross-site scripting (XSS)
	· Cross Site Request Forgery
	· SQL injection
	· Parameter and HPP tampering
	· Sensitive information leakage
	· Session highjacking
	· Buffer overflows
	· Cookie manipulation
	· Broken access control
	· Forceful browsing
	· Hidden fields manipulation
	· XML bombs/DoS
	· Open Redirect
	Debe poder identificar y configurar URLs que generen un gran consumo de recursos en los servidores como método de protección de ataques de denegación de servicios.
	Debe permitir verificaciones de seguridad y validación a protocolos FTP y SMTP
	Debe incluir firmas de BOTS para detectar y bloquear tráfico originado por estos.
	Debe soportar CAPTCHA como método de prevención para mitigar ataques de denegación hacia las aplicaciones protegidas.
	Debe ofrecer protección sobre tráfico basado en WebSockets
	El equipo debe soportar la implementación de VPN SSL (FUNCION ACCESO)
Estándares de Red	Soporte VLAN 802.1q, Vlan tagging
	Soporte de 802.3ad para definición de múltiples troncales
	Soporte de NAT, SNAT
	Soporte de IPv6: El equipo debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente.
	Soporte de Rate Shapping.
	Soporte de dominios de Enrutamiento, donde cada uno pueda tener su propio Default Gateway y estar conectados a redes IP con el mismo direccionamiento.
	Debe soportar protocolos de enrutamiento BGP, RIP, OSPF, IS-IS

	La solución debe permitir el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH, interfaz de administración gráfica basada en Web seguro (HTTPS)
	La solución debe integrarse con LDAP, para la autenticación de usuarios para gestión de la herramienta.
	La solución debe integrarse con RADIUS y TACACS+ para la autenticación de usuarios para gestión de la herramienta.
	La solución debe incluir comunicación cifrada y permitir la autenticación del equipo y de los usuarios administradores/supervisores con Certificados Digitales
	La solución debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante:
	· Protocolo SysLog
	· Notificación vía SMTP
	· SNMP versión.2.0 o superior.
Administración del Sistema	El sistema de administración debe ser totalmente independiente del sistema de procesamiento de tráfico.
	El equipo debe contar con un módulo de administración tipo lights out que permita encender/apagar el sistema de manera remota y visualizar el proceso de arranque.
	La interfaz gráfica debe contar con un Dashboard personalizable que permita monitorear el estado del equipo en tiempo real
	Debe contar con un módulo de reportes que permita visualizar gráficamente el comportamiento de las aplicaciones HTTP como latencias hacia los servidores, latencias en los URL, Direcciones IPs que acceden las aplicaciones, URLs más visitados en las aplicaciones, Throughput hacia los servidores y estadísticas acerca de los servicios creados y los servidores físicos.
	Debe Contar con plantillas para la implementación rápida de aplicaciones de mercado conocidas (ej, Oracle, Microsoft, SAP, IBM) y permitir crear plantillas personalizadas que puedan ser actualizadas/exportadas entre equipos.
Virtualización	Cada equipo debe soportar virtualización del dispositivo que soporte mínimo 4 instancias del sistema operativo corriendo simultáneamente, cada una con CPU y Memoria independientes, las cuales deberán ser configuradas de acuerdo a la migración de las actuales plataformas.
	Cada instancia virtual debe permitir ejecutar su propia versión de sistema operativo y no ser compartido entre instancias virtuales.
	Cada instancia debe manejar su alta disponibilidad de manera independiente para así poder garantizar la alta disponibilidad en caso de control de cambios.

	Cada instancia virtual debe soportar dominios de enrutamiento, donde dominio pueda tener su propio Default Gateway y estar conectados a redes IP con el mismo direccionamiento
	La solución deberá tener la capacidad de soportar en cada instancia capacidades distintas o iguales depende del diseño que será propuesto por la entidad en recomendación con el fabricante que sea propuesto por el oferente.
Redundancia en fuente de poder	El equipo debe soportar fuentes de poder redundantes internas, con la característica de instalación en caliente (hot-swap/plug).
	Debe incluir fuentes de poder redundantes AC.
Ventilación	Debe tener sistema de ventilación redundante y hot-swap/plug

Actividad 1.2 Adquisiciones de los equipos de seguridad firewall perimetral y firewall IPS de data center para el Centro de Datos Principal

El presente proyecto busca el reemplazo de los equipos de seguridad firewalls, mediante la implementación de equipos con vigencia tecnológica y que sean compatibles con las configuraciones actuales, de manera que las aplicaciones no se vean afectadas con el cambio.

Las actividades de reemplazo de los equipos de seguridad firewalls deben realizarse con el mínimo impacto y manteniendo la operatividad de las Aplicaciones del SINFIP.

Para lo cual se requiere:

- Adquirir 2 equipos firewalls de seguridad perimetral para el Centro de Datos Principal, con las siguientes características:

Tabla 35 Especificaciones técnicas Equipos firewalls de seguridad perimetral

ESPECIFICACIONES	REQUERIMIENTO MANDATORIO
Cantidad	2 (dos)
Fabricante	Especificar
Modelo	Especificar
Año de fabricación	>=2022
Procedencia	Nuevo de Fábrica. No se aceptarán equipos remanufacturados
Tipo	NGFW para seguridad Perimetral en alta disponibilidad (HA)
Throughput	Cada dispositivo debe proporcionar:
	Throughput de Next generation firewall >=10 Gbps publicado en el datasheet y

	Throughput de Threat Prevention >= 5 Gbps publicado en el datasheet
	El parámetro solicitado, debe ser medido con tráfico productivo real (Transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP de 64KB de tamaño).
	No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.
Conexiones Concurrentes	Cada equipo debe soportar >= 1.4 millones de conexiones concurrentes en control de aplicaciones.
Nuevas conexiones por segundo	Cada equipo debe soportar >= 30.000 nuevas sesiones o conexiones por segundo en control de aplicaciones
Interfaces de Administración	Cada equipo debe contar con 1 interface 10/100/1000 Mbps para comunicación con el sistema de gestión.
Puertos USB	Cada equipo debe contar con >=1 puerto USB 2.0.
Puertos de Consola	Cada equipo debe contar con un puerto serial de consola RJ-45.
Cantidad de Interfaces	Incluir >=8 interfaces de cobre a 1 Gbps RJ45
	Incluir >=4 interfaces de fibra de 10Gbps con sus respectivos transcerivers SFP+ SR (LC)
	Incluir sus respectivos patchords de fibra
Cantidad de Usuarios	Deben soportar una cantidad de usuarios ilimitados en modo Firewall.
Almacenamiento	Cada equipo debe contar con >=1 disco de estado sólido de >=200 Gb.
Alimentación Eléctrica	Redundante, 100 a 240 VAC, 50 a 60 Hz.
Redundancia en fuente de poder	Debe soportar fuente de poder redúndate hot-swappable, AC
Funcionalidades requeridas licenciadas	· NGFW.
	· IPS
	· VPNs
	· Antimalware.
	· Aplication Control
	· Filtrado de URLs
	· Filtrado de Contenido
	· Sandbox o Equivalente

- Adquirir 2 equipos firewalls IPS para data center, para la seguridad de las aplicaciones, con las siguientes características:

Tabla 36 Especificaciones técnicas Equipos firewalls IPS para data center

ESPECIFICACIONES	REQUERIMIENTO MANDATORIO
Cantidad	2 (dos)
Fabricante	Especificar
Modelo	Especificar
Año de fabricación	>=2022
Procedencia	Nuevo de Fábrica. No se aceptarán equipos remano facturados,
Tipo	NGFW para seguridad Perimetral en alta disponibilidad (HA)
Throughput	Cada dispositivo debe proporcionar:
	Throughput de Next generation firewall >=14 Gbps publicado en el datasheet y
	Throughput de Threat Prevention >= 12 Gbps publicado en el datasheet
	El parámetro solicitado, debe ser medido con tráfico productivo real (Transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP de 64KB de tamaño).
	No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.
Conexiones Concurrentes	Cada equipo debe soportar >= 3 millones de conexiones concurrentes en control de aplicaciones.
Nuevas conexiones por segundo	Cada equipo debe soportar >= 90.000 nuevas sesiones o conexiones por segundo en control de aplicaciones
Interfaces de Administración	Cada equipo debe contar con 1 interface 10/100/1000 Mbps para comunicación con el sistema de gestión.
Puertos USB	Cada equipo debe contar con 1 puerto USB 2.0.
Puertos de Consola	Cada equipo debe contar con un puerto serial de consola RJ-45.
Cantidad de Interfaces	Cada equipo debe contar con
	Incluir >=8 interfaces de cobre a 1 Gbps Rj45-
	Incluir >=8 interfaces de fibra de 10 Gbps con sus respectivos transcerivers SFP+ SR (LC)
	Soportar al menos dos interfaces de 40 Gb.
	Incluir sus respectivos patchords de fibra
Cantidad de Usuarios	El equipo debe soportar una cantidad de usuarios ilimitados en modo Firewall.
Almacenamiento	Cada equipo debe contar con >= 1 disco de estado sólido de 200GB.
Alimentación Eléctrica	Redundante, 100 a 240 VAC, 50 a 60 Hz.
Redundancia en fuente de poder	Debe soportar fuente de poder redúndate hot-swappable, AC
Funcionalidades requeridas licenciadas	NGFW
	IPS

Tabla 37 Especificaciones para funcionalidades de seguridad requeridas firewalls perimetral y datacenter

FUNCIONALIDAD A NIVEL DE FIREWALL	
Mecanismos de Control	Debe soportar control basado en técnicas de "statefull inspection"
Filtrado de Tráfico	Debe soportar mecanismos de filtrado de tráfico basado: dirección IP, protocolo, puertos y otros.
	Debe permitir crear políticas Direcciones IP, redes y zonas de seguridad, Dominio (FQDN), por usuario, grupos de usuarios.
	Permitir especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora)
Mapeo de Direcciones y Puertos	Debe contar con capacidad para integrar esquemas de red NAT/PAT (Network Address Translation/Port Address Translation).
	Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP.
Disponibilidad	Deberá de soportar mecanismos de alta disponibilidad: Activo/pasivo o Activo/Activo.
Direccionamiento	Deberá soporta direccionamiento IPv6 basado: direccionamiento en interfaces; IPv6 lista de acceso; IPv6 rutas estáticas.
Bloqueo de tráfico por geolocalización	Cada equipo debe permitir y/o bloquear tráfico por geolocalización; ya sea por país o continente
Protocolos Multicast	debe soportar Protocol Independent Multicast (PIM) e Internet Group Management Protocol (IGMP) para aplicaciones tipo multicast.
Políticas de Calidad de Servicio	Debe permitir la configuración de políticas de calidad de servicio y rate limit bajo las siguientes características: por protocolo, ancho de banda, tanto para tráfico de entrada como de salida, por IP o red
Filtrado de URL	La solución debe manejar categorización de URLs.
	La solución debe permitir crear reglas de filtrado con múltiples categorías.
	Se requiere que la creación de una nueva regla cuente con por lo menos las siguientes acciones:
	Para control de aplicaciones bloquear, monitorear (registrar el log).
	Para filtrado de URL: bloquear, monitorear (registrar el log).
	La solución debe categorizar las aplicaciones por factor de riesgo.
	Debe ser posible definir la política de seguridad de aplicaciones y URLs basada en identidades de usuario.
	La base de datos de aplicaciones y URLs debe ser actualizada por un servicio basado en la nube.
	La solución debe incluir un mecanismo para informar al usuario final las violaciones de las políticas de seguridad.
	La solución debe ofrecer opciones para modificar las páginas o notificaciones de bloqueo y para redireccionar al usuario a una página de remediación.

	La solución debe incluir un contador de hits que muestre el uso de cada regla.
	Debe detectar y bloquear aplicaciones que realizan Comando y Control.
	Debe ser posible crear expresiones regulares para bloquear sitios de manera personalizada.
	Debe contar con multi categorías de URL, que permita que un sitio web pertenezca a dos categorías distintas.
FUNCIONALIDAD A NIVEL DE CONTROL DE APLICACIONES	
Filtrado de Aplicaciones	Debe permitir filtrar aplicaciones por aplicación y Categorías
	Debe ser posible definir nuevas aplicaciones, así como categorías que no estén definidos dentro de la base de datos del fabricante.
	Debe poder controlar las aplicaciones en cualquier puerto.
Aplicaciones Detectadas	Debe detectar >= 4000 aplicaciones y categorizarlas tipo y por riesgo.
Reglas de Control de Aplicaciones	Debe permitir la creación de reglas para controlar el uso de aplicaciones a través de las siguientes condiciones: Direcciones IP, redes y zonas de seguridad, por usuario, grupos de usuarios
	Debe usar al menos las siguientes acciones en una regla de control de aplicaciones: bloquear, permitir, informar al usuario.
Integración LDAP	soportar integración a través del directorio activo y/o LDAP para hacer reglas basadas en identidad
HTTPs Inspection	Debe inspeccionar el tráfico HTTPS, con el fin de prevenir riesgos de seguridad relacionados con el protocolo TLS.
FUNCIONALIDAD A NIVEL DE VPN	
VPN IPSeC	Debe soportar VPNs Site-to-site basadas en IPSec.
	Debe soportar VPNs client-to-site basadas en IPSec.
	Debe permitir ilimitadas VPN IPSEc site to site
	Debe permitir 50 usuarios vpn ipsec y ssl
VPN SSL	Debe soportar VPN SSL con o sin agente.
	Debe soportar VPN SSL desde dispositivos móviles (S.O. Android y IOs)
	Incluirá un método simple y centralizado para crear túneles permanentes entre Gateways del mismo fabricante.
VPN CON MFA	Debe soportar autenticación de doble factor (MFA)
FUNCIONALIDAD A NIVEL DE PREVENCIÓN DE INTRUSOS (IPS)	
IPS	La plataforma propuesta por el fabricante debe contar con certificación USGv6 para trabajar IPv6 tanto en Firewall como en IPS.
Protocolos	Inspección con firmas de IPS de al menos los siguientes protocolos SQL, LDAP, HTTP, DNS, SMTP POP3, IMAP, SMB, FTP, SSH

Monitoreo por Segmentación	Debe ser capaz de inspeccionar el tráfico asociado a distintos segmentos de redes diferentes (en lugar de tener una sola política por interfaz).
Niveles de Políticas	Debe permitir controlar políticas a nivel de, puerto, subred y direcciones IP.
HTTP ofuscación	Debe ser resistente a diversas técnicas de obfuscation y evasión
Reglas de Detección de lenguaje abierto	Debe soportar reglas de detección basada en un lenguaje abierto permitiendo a los usuarios crear e importar sus propias reglas.
Respuestas Frente a Amenazas	Debe soportar los siguientes tipos de acciones: bloquear p prevenir, detectar o monitorear, ignorar o inactivar.
Protección VoIP	Soportar la identificación y protección de ataques en protocolos de Voice over IP (VoIP) sobre SIP.
URL ofuscación	Debe ser resistente a diversas técnicas de ofuscación y evasión
Análisis de paquetes IPv4 e IPv6	Cada equipo debe tener la habilidad de decodificar e inspeccionar todos los protocolos apoyados IPv4, y cualquier ataque asociado o mal uso incluso si está encapsulado en IPv6.
Captura de tráfico	Cada equipo debe poder realizar capturas de tráfico para el análisis de evidencia en formato soportado por TCPDUMP y PCAP (estándar para el software de análisis de protocolos).
Integración LDAP	Debe soportar la integración a través del directorio activo y/o LDAP para hacer reglas basadas en identidad
Firmas de IPS por Plataforma	Cada equipo debe poder soportar selección de firmas de IPS por plataforma tal como: Apple; Cisco; HP; IBM; Juniper; Microsoft; RedHat; Suse; Sun para usarlas en reglas de seguridad
Reglas para Excepciónes	Debe tener la capacidad de crear reglas de excepción para que el tráfico no sea inspeccionado
Creación de objetos	Debe soportar la creación de objetos por nombre ya sea por: network, puertos, subred, URL, y zonas de seguridad.
Protección de Aplicaciones Web	Debe proteger contra ataques sobre aplicaciones Web como: shell command injections, Server-site injection, cross-site scripting, directory traversal.
Detección de anomalías en el tráfico de red	Deberá ser capaz de detectar anomalías de tráfico en la red, en base a los patrones de tráfico identificados.
Búsqueda de firmas	Debe soportar la búsqueda de firmas por nombre a través de la interfaz gráfica.
Filtros de protección	Debe soportar filtros que protejan las vulnerabilidades de navegador web.
Firmas de vulnerabilidades	Debe estar basado sobre firmas en vulnerabilidades permitiendo la detección variaciones de ataques conocidos, con capacidad para detectar software malicioso que se aprovecha de vulnerabilidades conocidas
HTTPs Inspection	Debe inspeccionar el contenido de tráfico HTTPS, con el fin de prevenir riesgos de seguridad relacionados con ataques cifrados
FUNCIONALIDAD A NIVEL DE PROTECCIÓN DE MALWARE	

Prevención de Amenazas	Debe proteger a la institución contra ataques cibernéticos de malware, Botnets
Protección hacia el Internet	La solución debe proporcionar detección y protección en las comunicaciones desde y hacia los servicios de internet, contra los ataques de malware, exploits, botnets
IP Reputation	Debe contar con IP, URL y Domain Reputation para: Bots, CnC y Malware,
	Debe permitir bloquear dominios potencialmente maliciosos de acuerdo a su comportamiento
	Debe permitir bloquear de forma automática dominios/url maliciosos que esté en la lista negra de la base de datos del fabricante
Nube de Seguridad del Fabricante	La solución debe utilizar una nube que le permita beneficiarse de la información recogida por los esfuerzos de investigación del fabricante.
	Permitir la subida de archivos al sandbox de forma manual y vía API
Capacidad de Detección de Tráfico cifrado y no cifrado	Para hacer la inspección la solución debe trabajar en base a los siguientes protocolos: HTTP, HTTP/2 FTP,DNS, SMTP, POP3, IMAP y SMB (versiones 1, 2 y 3). Tanto en IPv4 como en IPv6
Comando y Control (callbacks)	La solución debe tener la capacidad de bloquear llamadas a servidores remotos (Callbacks, llamadas de Comando & Control). Protegiendo los equipos que pudiesen haberse comprometido y se encuentren realizando llamadas a servidores remotos desde la red corporativa.
	Debe hacer inspección sobre tráfico encriptado SSL/TLS v1.3.
Descarga de Archivos	La solución debe proporcionar protección contra ataques originados en la web, como descargas de archivos maliciosos
Personalizar Reglas	La herramienta debe ser capaz de soportar la importación de reglas personalizadas.
Detección Origen direcciones IP de ataques	La solución debe permitir la identificación de las direcciones IP de origen de los ataques (geo-localización).
Estadísticas de Infección	La solución será capaz de proporcionar información de cuantas veces un equipo ha sido infectado y bloqueada la comunicación. Así como también del Malware que lo ha infectado
Por cada una de las infecciones por malware detectadas, se deberá mostrar los siguientes campos	EL HASH de la descarga SHA o MD5, IP origen e IP destino,
	Poder agregar a listas personalizadas o de exclusión. Guardar una captura del archivo, malicioso, en función de las políticas definidas.
Prevención de Amenazas Avanzadas	Deberá emular los archivos sospechosos en entornos (Windows, Linux, Android, Mac) o emular más de 80 tipos de archivos.
	La solución debe proveer la habilidad de analizar y detectar código malicioso (malware) en documentos de Adobe PDF y archivos de Microsoft Office, así como también archivos EXE, ZIP, Flash, Java.
	Debe incluir un servicio de analítica y machine learning para amenazas avanzadas.

- Adquirir 1 equipo de administración para firewall de siguiente generación

Tabla 38 Especificaciones técnicas equipo de administración para firewall

ESPECIFICACIÓN	REQUERIMIENTO MANDATORIO
Cantidad	1 (un)
Fabricante	Especificar
Modelo	Especificar
Año de fabricación	>=2022
Procedencia	Nuevo de Fábrica. No se aceptarán equipos remanufacturados
Interfaces de Red	debe contar con al menos 1 interface 10/100/1000 Mbps para comunicación con el sistema de gestión.
	debe contar con >=2 interfaces 10Gb con sus respectivos SFP y fibras ópticas para conectividad
CPU	debe contar con >=8 CORES
MEMORIA	debe contar con >=64 GB
Almacenamiento de eventos	debe contar con >=2 discos que utilice un mecanismo redundante por lo menos RAID 1 de 1.8 TB.
Alimentación Eléctrica	Redundante, 100 a 240 VAC, 50 a 60 Hz.
Redundancia en fuente de poder	Debe soportar fuente de poder redúndate hot-swappable, AC
Funcionalidades requeridas	Administración
	Monitoreo
	Logs y eventos de seguridad
	Reportes de seguridad
	Monitoreo de cumplimiento de estándares y mejores prácticas de seguridad
	Debe soportar 40 Millones de eventos IPS
Administración	La solución debe soportar consola remota con interfaz gráfica, a, perfiles para diferentes de usuarios.
Detalle del Estado del Hardware de los distintos equipos de seguridad	Es importante que el sistema de administración centralizada cuente con herramientas integradas para tener visibilidad en forma de graficas en tiempo real e historial sobre el estado de salud, como mínimo de: CPU, interfaces, memoria, performance, disco, temperatura.
Visibilidad de Software y Hardware	El sistema de administración debe proveer la capacidad de visualizar las versiones de software y hardware de los equipos desde la consola principal
Monitoreo de Gateways	Debe permitir visualizar el estado de los tuneles VPN y de los usuarios remotos que están conectados a los gateways.
Integración a través de APIs	La solución debe incluir un mecanismo de integración, en forma de APIs abiertas y / o interfaces estándar, para permitir insertar feeds de terceros o indicadores de compromiso de amenazas identificadas de forma externa.

	La solución debe incluir un mecanismo de integración, en forma de APIs abiertas y / o interfaces estándar, para permitir a los eventos y registro de datos sean compartidos con la red externa y las aplicaciones de gestión de seguridad, tales como sistemas de ticketing, SIEM, plataformas de sistemas de gestión y registro de las herramientas de gestión.
Cumplimiento	La solución debe ser capaz de crear perfiles de cumplimiento con alguna normativa de seguridad para emitir una alarma cuando se tenga configura alguna mala práctica por una normativa de seguridad (ejemplo ISO 27001)
Dashboard	La solución que permita personalizar la información presentada en él acerca de amenazas, servicios de comando y control, posibles firmas asociadas, severidad y otros campos, y poder generar un reporte a partir de este Dashboard personalizado.
Detalles de Amenazas	La solución debe contar con información detallada de ayuda para firmas. Cuando aparece una amenaza en la pantalla de la consola, el usuario debe tener la capacidad de visualizar información detallada acerca de la vulnerabilidad hacia la cual está dirigida la amenaza. Ello debe incluir una explicación de la vulnerabilidad, de los sistemas que pueden verse afectados, de información CVE.
Visibilidad de la red a proteger	La solución debe permitir Visibilidad del tráfico de red incluyendo al menos lo siguiente parámetros: Redes; Host, Servicios; Aplicaciones; Firmas de IPS
	La solución debe soportar la correlación de múltiples eventos identificados como un único ataque.
Consulta de Históricos	La solución debe permitir consultar un histórico de los eventos sucedidos en los NGFW desde la consola principal, con el fin de realizar análisis forense.
	Cada equipo debe ser capaz de proporcionar mayor visibilidad sobre cómo se consume el ancho de banda, ya sea por dirección, puerto y aplicación.
Visibilidad de la red a proteger	La solución debe permitir Visibilidad del tráfico de red incluyendo al menos lo siguiente parámetros: Redes; Host, Servicios; Aplicaciones; Firmas de IPS
Tipos de Reportes	La solución deberá permitir reportes para las funcionalidades requeridas de FW, VPN, APPLICATION CONTROL, ANTIMALWARE, detallados sobre lo siguiente: Uso de tráfico por aplicación; Uso de tráfico por usuario; Uso de tráfico por host; Uso de tráfico por servicio; Eventos de seguridad por criticidad de la vulnerabilidad. Los reportes deben ser personalizables a las necesidades de la institución.
	Reportes en un rango de fechas y rango de direcciones IP.
Formatos de Reportes	La solución debe soportar reportes en formato texto y gráfico, con exportación en los formatos, PDF e CSV.
Reportes vía Correo	La solución debe generar reportes en forma automática y enviarlos a una cuenta de correo electrónico para agilizar el proceso de análisis.

Actividad 1.3 Adquisición de infraestructura para el reforzamiento de conectividad LAN del Centro de Datos principal del Ministerio de Economía y Finanzas

La presente contratación busca el reforzamiento y la alta disponibilidad de las comunicaciones que soportan a los sistemas del Ente Rector, mediante la implementación de otro equipo de comunicaciones para ser configuración requerida, de manera que las aplicaciones no se vean afectadas con el cambio.

Para lo cual se requiere:

- Adquirir 1 switch core compatible de forma nativa con el Switch de Core LAN actual HPE Aruba 8400 propiedad del Ministerio de Economía y Finanzas con las siguientes características:

Tabla 39 Especificaciones técnicas Switch Core

ESPECIFICACIONES	REQUERIMIENTO
Cantidad	1 (uno).
Marca	Indicar.
Modelo	Indicar
	Compatible de forma nativa con el Switch de Core LAN actual HPE Aruba 8400 propiedad del Ministerio de Economía y Finanzas con el cual se debe formar un cluster en alta disponibilidad, de modo que se comporten como un solo dispositivo virtual en capa 2.
Año de fabricación	>=2022
Procedencia	Nuevo de fábrica. No se aceptarán equipos re manufacturados.
Tipo	Red de LAN basada en equipos switch del tipo “Core”, modular. No bloqueante.
Requerimientos técnicos	Switch de capa 2, 3 avanzado
	Switch LAN que garantice una disponibilidad de 99,999%.
	El equipo debe incluir al menos dos (2) bahías para módulos de administración.
	Los módulos de administración deben operar al menos en modo activo/pasivo.
	La solución debe tener instalado al menos dos (2) módulos de administración.
	El equipo debe tener >= ocho (8) bahías para módulos de Entrada/Salida (I/O). Cada bahía para módulos de I/O debe ofrecer una capacidad de conexión de al menos 1.2Tbps.
	El equipo deberá soportar 8 módulos de Entrada/Salida (I/O) con puertos de 10 GbE, 25GbE, 40 GbE y 100 GbE.

	El equipo debe incluir >= (5) cinco módulos de Entrada/Salida (I/O):
	· 4 módulos de Entrada/Salida (I/O) con >= 32 puertos de 1/10 GbE SFP+
	· 1 módulos de Entrada/Salida (I/O) con >= 8 puertos de 40GbE QSFP+.
	El equipo ofertado deberá soportar una funcionalidad de stacking o cluster de switching entre mínimo dos (2) switches del mismo modelo a través de una conexión física.
	Los equipos que son parte del cluster o stack deberán comportarse como un dispositivo virtual en Capa 2.
	La conexión de los equipos debe ser a través de interfaces estándar de 10GE, 25GE, 40GE, 100GE o de enlaces dedicados.
	Proveer todo el Hardware y software necesario para conectar el equipo propuesto con el Switch de Core LAN actual HPE Aruba 8400 propiedad del Ministerio de Economía y Finanzas mediante al menos dos (2) enlaces de 5m a 40GE cada uno y un (1) enlace para keepalive a 10GE.
	Debe incluir Interfaces:
	• 10GbE >= 126 transceivers SFP+ SR (fibra multimodo, para alcance de hasta 300m) con sus respectivos cables de fibra.
	Debe incluir al menos Interfaces 40 GbE:
	• >= 4 transceivers 40G QSFP+ MPO SR4 (fibra multimodo, para alcance de hasta 150m) con sus respectivos cables de fibra.
	Debe ofrecer una capacidad al menos de:
	• Rendimiento: 7.142 Bpps.
	• Capacidad de conmutación: 19,200 Gbps (19.2 Tbps).
	Memoria RAM >= 16 GB.
	Memoria FLASH o SSD >= 32 GB.
	El sistema operativo debe incluir la última versión completa, liberada por el fabricante a la fecha de la compra, con todos los protocolos, servicios y funcionalidades que el equipo sea capaz de realizar.
Administración y monitoreo	Consola:
	• >=1 RJ45 puerto serial de consola.
	• >=1 RJ45 puerto serial de consola.
	• >=1 puerto USB.
	Acceso y configuración mediante:
	• Línea serial de comandos (CLI)
	• SSH v2

	Debe soportar múltiples configuraciones almacenadas en la memoria flash o en el SSD.
	Al menos debe soportar los siguientes protocolos:
	• SNMP v1, v2c, v3
	• sFlow (RFC 3176)
	• NTP
	• RMON
	Debe soportar Mirroring:
	• Al menos cuatro grupos sin restricción en el número de puertos por grupo.
Requerimientos L2	Tamaño de las tablas >=768.000 direcciones MAC.
	Debe soportar VLANs
	• >=4094 VLAN ID simultáneos
	• Enrutamiento inter VLAN.
	Debe soportar servicios y funcionalidades para L2: Detección de estado de canales.
	Soporte de tramas de hasta 9000 bytes
	Debe soportar al menos Protocolos y Estándares
	• IEEE 802.1Q.
	• IEEE 802.1w.
	• IEEE 802.1p.
	• IEEE 802.3x.
	• IEEE 802.3z.
	• IEEE 802.3ab.
	• IEEE 802.3ac.
	• IEEE 802.3ad.
	• IEEE 802.3ae.
	• IEEE 802.3ba.
	Listas de Acceso/Listas de control de acceso (ACL) en todos los puertos:
	• Parámetros configurables de Capa 2, Capa 3 y Capa 4.
	• VLAN ACL
	• Port ACL
	Link Agregación:
	• LACP IEEE 802.3ad:
	• Estático / Dinámico.
	• >= 128 grupos.
	• >=8 interfaces por grupo.
	Debe soportar:
	• STP
	• RSTP

	• MSTP
Requerimientos L3	Debe incluir enrutamiento básico y avanzado (Protocolos enrutados):
	• Ipv4
	• Ipv6
	Tamaño de las tablas: debe incluir para los protocolos de enrutamiento:
	• >=60,000 rutas unicast Ipv4.
	• >=8,000 rutas Ipv6.
	Debe incluir los siguientes protocolos para Ipv4 e Ipv6
	• Enrutamiento: estático, OSPF, BGP.
	• Policy Routing.
	• OSPFv3
	• VRRP.
	• Enrutamiento Inter-Vlan.
	• IP helper
	Debe soportar ARP
	• Estático
	• Protección de ataques ARP
	• ARP local proxy.
	• Gratuitous ARP.
	Debe soportar manejo de rutas: Equal-Cost Multipath, habilita múltiples enlaces de igual costo para incrementar la redundancia y escalabilidad.
	Debe incluir Multicast:
	• IGMP (Internet Group Management Protocol) v1, v2 y v3.
	• IGMP Snooping.
Requerimientos QoS	Data Center Bridging (DCB)
	Priority Flow Control (PFC)
	Enhanced Transmission Service (ETS)
	DCB Exchange Protocol (DCBX)
	Explicit Congestion Notification (ECN)
	Packet storm protection
Requerimientos Seguridad	Debe soportar Autenticación:
	• Autenticación vía RADIUS server.
	• TACACS+
	Debe soportar Servicios de seguridad:
	• Certificados internos auto firmados
	• TAA compliance con FIPS 140-2
	• Ethernet Ring Protection
	• Debe soportar Alta disponibilidad

Alta disponibilidad	Incluir 2 cables Direct Atach para conexión a 40 Gb y de >= 5 metros
	Incluir 2 cables Direct Atach para conexión a 10 Gb y de >= 5 metros
Instalación Física	El equipo será instalado en el Centro de Datos del Ministerio de Economía y Finanzas en un rack estándar de 42U que posee la institución.
	El oferente debe incluir los accesorios necesarios para su montaje en rack estándar de 19 pulgadas.
Alimentación eléctrica y ventilación	Redundante, 100 – 140 / 180 – 260 VAC, 50 a 60 Hz.
	El oferente debe incluir unidades de distribución de energía (PDUs) para la cantidad de corriente que consumirá la solución a 220 voltios, dividido en circuitos independientes, cada uno con interruptores de corriente (breakers) de protección.
	Los conectores eléctricos de las PDUs deben ser del tipo 2 fases y tierra. El oferente deberá proveer los conectores para cada uno de los circuitos de ser necesario.
	Incluir 3 fuentes de poder AC que se puedan remover en caliente (hot-swap)
	Incluir:
	• Ventilación Delante hacia Atrás.
	• >= 18 ventiladores redundantes.

- Upgrade del Switch Core LAN de propiedad del MEF

Tabla 40 Especificaciones técnicas Upgrade Switch Core

ESPECIFICACIÓN	REQUERIMIENTO
Cantidad	N/A
Marca	Indicar. El hardware ofertado debe ser compatible con el Switch Core LAN HPE Aruba 8400 que posee actualmente el Centro de Datos Principal del Ministerio de Economía y Finanzas.
Modelo	Indicar
	Los módulos, piezas y partes deben ser liberadas para la venta por el fabricante y que cumpla con las especificaciones técnicas indicadas.
Año de fabricación	>=2022
Procedencia	Nuevo de fábrica. No se aceptarán equipos re manufacturados.
Tipo	Módulos de Entrada/Salida (I/O)

Características Físicas y de Rendimiento	Se requieren (2) dos módulos de Entrada/Salida (I/O) para incremento de capacidad de conmutación del switch core LAN existente:
	· 2 módulos de Entrada/Salida (I/O) y cada módulo con >= 32 puertos de 1/10 GbE SFP+.
	Cantidad de Interfaces incluidas:
	· 10 GbE >= 64 transceivers SFP+ SR (fibra multimodo, para alcance de hasta 300m) con sus respectivos cables de fibra.
Alta disponibilidad Switch de Acceso	Se requiere 1 cable de conexión directa que incluya los conectores en los extremos para brindar conexión a 10Gb cada uno. (Direct Atach).
	Distancia mínima de los cables >= 5 metros

- Adquirir 3 Switches de acceso

Tabla 41 Especificaciones técnicas 3 Switches de acceso

ESPECIFICACIÓN	REQUERIMIENTO
Cantidad	Tres (3)
Marca	Especificar / Compatible con el equipo switch core LAN actual propiedad del MEF.
Modelo	Especificar
Año de Fabricación	>=2022, no remanufacturados, no reconstruidos, no reacondicionado.
Tipo	Tamaño fino 1 RU.
Capas	Switch de capa 2, 3
Sistema Operativo	El sistema operativo debe incluir la última versión completa con todos los protocolos, servicios y funcionalidades que el equipo sea capaz de realizar liberada por el fabricante a la fecha de la compra.
Puertos para datos	Cada equipo debe incluir al menos:
	· 48 puertos 10/100/1000Base-T Auto-MDIX.
	· 4 puertos de 1GE/10GE SFP/SFP+
	Todos los interfaces deben estar habilitados, activos y listos para su uso. El proveedor deberá incluir todo el licenciamiento que el equipo requiera para cumplir esta condición.
Puertos para administración	Al menos:
	· 1 puerto serial de consola.
	· 1 puerto Ethernet RJ45 para administración fuera de banda.
	· 1 USB para administración de archivos.

Transceiver 10GBE	Incluir al menos: · 4 transceivers SFP+ SR (en total).
Rendimiento	Al menos: · Rendimiento: 130 Mpps · Capacidad de conmutación: 176 Gbps. El equipo debe ser no-bloqueante en todos sus interfaces.
Latencia	Máximo: · 2.3 microsegundos en 1Gbps. · 1.5 microsegundos en 10Gbps.
Memoria	Al menos: · FLASH/eMMC: 16 GB. · RAM: 8 GB. · Packet Buffer: 8 MB.
Administración y Monitoreo	
Protocolos y servicios para Gestión	Al menos vía: · Administración a través de línea de comandos CLI. · Administración a través de un puerto Ethernet fuera de banda. · SSHv2 y SSHv6. · SNMPv2c y SNMPv3. · Administración y monitoreado a través de un software de gestión externo del mismo fabricante del switch, el cual al menos muestre de manera gráfica, estadísticas, alarmas, topología y permita realizar configuraciones. · Administración desde un servicio en nube. · sFlow · NTP · RMON · SFTP · TFTP
Sistema Operativo y Configuraciones	Soporte al menos: · Múltiples configuraciones almacenadas en la memoria. · Descarga de software desde el puerto USB. · Capacidad de almacenar dos imágenes de sistema operativo.
IPv6	Soporte al menos de: · Ping para IPv6 · Traceroute para IPv6
Mirroring	Soporte de al menos:

	· Duplicación (mirroring) de tráfico de ingreso y egreso de un interfaz.
	· Al menos 4 grupos.
Requerimientos L2	
Tamaño de las tablas	Al menos:
	· 16.000 direcciones MAC.
VLANs	Al menos:
	· 4000 VLAN IDs.
	· 2000 VLAN simultáneas.
Tramas	Soporte de tramas de al menos 9198 bytes.
Protocolos y Estándares	Al menos:
	· IEEE 802.1Q.
	· IEEE 802.1w.
	· IEEE 802.1p.
	· IEEE 802.1s.
	· IEEE 802.1x.
	· IEEE 802.1ab.
	· IEEE 802.1ak.
	· IEEE 802.1ax.
	· IEEE 802.3x.
	· IEEE 802.3z.
	· IEEE 802.3ad.
	· IEEE 802.3ae.
	· IEEE 802.3af.
	· IEEE 802.3at.
Listas de Acceso	Al menos Listas de Control de Acceso (ACL):
	· Parámetros configurables de Capa 2, Capa 3 y Capa 4.
	· ACL para IPv4 e IPv6.
	· ACL para puertos.
	· ACL para VLAN.
Link Aggregation	LACP IEEE 802.3ad:
	· Estático / Dinámico
	· Al menos 32 agregados.
	· Al menos 8 puertos por agregado.
	· Soporte de algoritmo para hashing en L2 y L3.
Funcionalidades Capa 2	Soporte de:
	· STP
	· RSTP
	· MSTP

	· RPVST+
	· Detección de fallas en cables para evitar problemas de daño unidireccional.
Descubrimiento	Soporte al menos de:
	· LLDP
	· LLDP-MED
Clustering	Al menos capacidad de conectarse en cluster o stack con otro switch de la misma familia de switches:
	· Los equipos que son parte del cluster o stack deberán comportarse como un dispositivo virtual.
	· El cluster o stack debe ser capaz de crecer al menos hasta ocho (8) equipos.
	· La conexión de los equipos debe ser a través de interfaces estándar de 10GE, o de enlaces dedicados.
Requerimientos L3	
Protocolos enrutados	Al menos:
	· IPv4
	· IPv6
	· IPv4 IPv6 Dual Stack
Tamaño de las tablas	Al menos:
	· 2.000 rutas unicast IPv4
	· 1.000 rutas unicast IPv6
	· 1.000 grupos IGMP
	· 1.000 grupos MLD
Protocolos para IPv4	Al menos:
	· Enrutamiento: estático, RIPv2, OSPF.
	· VxLAN.
	· DHCP client.
	· DNS
	· IP Authentication Header
Protocolos para IPv6	Al menos:
	· Enrutamiento: estático, RIPng, OSPFv3.
ARP	Soporte de:
	· Modo estático.
	· Gratuitous ARP.ARP proxy.
Manejo de rutas	Al menos Equal-Cost Multipath para habilitar múltiples enlaces de igual costo.
Multicast	Al menos:
	· IGMP v1, v2 y v3.
	· IGMP Snooping.
	· MLD.
	· MLD Snooping.

QoS	
Control de tráfico de salida	Al menos soporte de limitantes de tráfico de egreso por puerto
Encolamiento	Al menos: · Strict Priority · Deficit WRR (DWRR)
Servicio	Al menos: · 802.1p · DiffServ · CoS · IP SLA
Control de tormentas	Al menos soporte de limitante de ingreso para tráfico de broadcast y multicast.
Seguridad	
Autenticación para administración	Soporte de: · Radius · TACACS+
Autenticación de usuarios	Soporte de: · Autenticación por dirección MAC · Radius · 802.1x · Autenticación basada en WEB desde portal cautivo externo.
Políticas basadas en roles	Integración con Sistema de Control de Acceso AAA para asignar políticas basada en el rol del usuario que se conecta, como ACL y VLAN.
Servicios de seguridad	Al menos: · Certificados internos auto firmados. · TAA compliance con FIPS 140-2.
Hardware y Energía	
Montaje	Debe traer todos los accesorios para montaje y operación en rack estándar de 19" de 4 postes.
Alimentación eléctrica	Soporte al menos: · AC 100-127 / 200-240 VAC. · 50 Hz a 60 Hz.
Ventilación	Ventilación Delante/Costado>Atrás (front/side-to-back).

Actividad 1.4 Adquisición de infraestructura y servicio para el reforzamiento de la nube privada

La presente contratación busca la adquisición e instalación de la infraestructura tecnológica para el reforzamiento de la Nube Privada propiedad de esta Cartera de Estado, que incluye la instalación del software base de los servidores solicitados e implementación de la Nube Privada en Windows Server Data Center 2019 o superior y servicios necesarios.

Para lo cual se requiere:

- 1 Rack

Tabla 42 Especificaciones Técnicas Rack

Rack	- El oferente deberá proveer un (1) rack de la misma marca de la infraestructura ofertada mismo que deberá cumplir mínimo con las siguientes características: - Rack de 42U, que cumpla la norma EIA-310. Paneles laterales, puertas delantera y posterior desmontables.

- 2 Chasis de servidores de última tecnología con las siguientes características:

Tabla 43 Especificaciones Técnicas de 2 Chasis

ESPECIFICACIÓN	REQUERIMIENTO MANDATORIO
Cantidad	- 2 (dos).
Marca	- Indicar. Ciento por ciento 100% compatible con la infraestructura procesamiento de cómputo de propiedad del Ministerio de Finanzas
Modelo	- Indicar
Año de Fabricación	- >=2022
Procedencia	- Nuevo de fábrica. No se aceptarán equipos remanufacturados.
Forma	- Tipo: Rack Altura: 10 unidades de rack por cada chasis
Configuraciones & Funcionalidades mínimas requeridas	- Capacidad mínima de 12 bahías para Módulos de Computo por Chasis. En caso no se cuente con lo solicitado, se podrá adicionar un segundo chasis de Módulos de Computo. - Capacidad de soportar Módulos de Computo con arquitecturas de procesadores Intel Xeon.

- El Chasis debe soportar módulos de cómputo de 2 y 4 procesadores físicos x86 (Intel Xeon) disponibles

- Debe soportar equipos de interconexión (módulos o switches) LAN de 100 GbE en los puertos externos y 50GbE en los puertos internos.

- Debe soportar equipos de interconexión (módulos o switches) SAN de 32 Gb Fibra Canal.

- El Chasis deberá de contar con indicadores físicos que permitan monitorear el estado de los diferentes componentes que alberga el mismo.

- Los módulos de cómputo a soportar deben ser capaces de guardar un log con todos los cambios de hardware ocurridos en el mismo. En caso de falla del módulo, será posible tener acceso a este log de forma remota y sin necesidad de sistema operativo en el módulo dañado.

- Para asegurar el crecimiento, el Chasis debe soportar hasta 960 cores físicos de procesamiento.

- La solución debe considerar una consola única para aprovisionar cómputo, almacenamiento externo y networking del lado de módulos de cómputo con opciones disponibles de DAS, iSCSI y FC SAN. Esta solución deberá tener alta disponibilidad.

- La solución deberá soportar un API que se integre a soluciones del mercado como Microsoft Systems Center, VMWare vCenter, VMware SDDC y también deberá permitir integración con soluciones de automatización y DevOps open source como Chef, Docker y OpenStack.

- La solución deberá soportar la creación de plantillas definidas por software que permitirán hacer cambios rápidos en la infraestructura. Las plantillas deben incluir BIOS del módulo de cómputo, firmware, boot order, RAID, configuración de storage y configuraciones de red requeridas para la carga de trabajo.

	- La solución deberá incluir SCRIPTS de integración con Dockers y otras plataformas de contenedores para la reasignación de recursos de cómputo, de almacenamiento externo y de red a diferentes cargas de trabajo para usar efectivamente la infraestructura.
	- El chasis debe tener la capacidad de manejar la infraestructura como código a través de Dockers, Chef, Puppet, Ansible y otros.
	- Soporte de soluciones tipo contenedores (containers) y gestión de los chasis como un pool de recursos gestionados a través del código de la aplicación.
	- Se debe contar con documentación y/o herramientas en GitHub de público acceso, que faciliten la integración e implementación de aplicaciones con la solución de infraestructura ofertada
	- El chasis debe ser capaz de aceptar la inserción en caliente de los servidores sin necesidad de interrumpir el servicio. Refiriéndose a la capacidad de insertar o retirar los servidores del chasis blade sin afectar o interrumpir el servicio de los demás servidores instalados dentro del chasis blade.
	- Se debe incluir 1 Rack y al menos dos PDUs del mismo fabricante del chasis para soportar la solución en su máxima capacidad.
Backplane	- El ancho de banda en el Chasis deberá de ser de 10 Tb como mínimo, también se aceptará soluciones que no usen backplane o midplane.
	- Debe incluir fuentes de poder hot-swap, load-sharing, load-balancing.
	- Debe poseer fuentes de poder de al menos 2400 watts de potencia.
	- Alimentación eléctrica de 220 VAC @ 60 Hz.
Fuente de Poder y Ventiladores	- No se deben utilizar transformadores externos.
	- Las fuentes de poder y los ventiladores deben ser redundantes y hot-swap.
	- Las fuentes de poder deben estar integrados en el Chasis y deberán permitir ser configuradas N+N.

	- Los ventiladores deben estar integrados en el Chasis y deberán permitir ser configuradas N+1.
	- Debe soportar la capacidad completa de todos los servidores instalados en el chasis operando sin limitar la potencia o el funcionamiento de los procesadores de cada módulo de cómputo.
	- Capacidad de soportar la interconexión simultánea de: Ethernet y Fibra Canal.
Interfaces I/O	- Debe contar con seis bahías como mínimo para equipos de interconexión.
	- Todos los módulos de interconexión de I/O deben ser intercambiables entre sí.
	- La solución deberá tener instalados al menos dos (2) módulos para la interconectividad LAN de 100Gbps y al menos dos (2) módulos para la interconectividad SAN de 32 Gbps.
	- Estos módulos de conectividad deberán permitir la conectividad de todos los módulos de Computo instalados sin impactar el rendimiento general de los Módulos de Computo o de la red.
Conectividad LAN y SAN	- Se deberá habilitar en los módulos LAN al menos 4 puertos de 40GbE externos para LAN por cada módulo como mínimo, incluir cada puerto con su respectivo transceiver y cable de fibra de 15 metros.
	- Se deberá habilitar en los módulos SAN al menos 4 puertos de 32Gb FC externos para SAN por cada módulo como mínimo, incluir cada puerto con su respectivo transceiver y cable de fibra de 15 metros.
	- Los módulos deberán soportar redes virtuales por puerto físico del módulo de cómputo y permitir administrar las direcciones físicas (MAC Address y WWN correspondientes) del mismo asignado a cada red virtual.
	- Deberán soportar la agregación (trunking) de conexiones hacia la infraestructura principal de redes LAN.

	- La administración de los módulos deberá ser transparente para el administrador de redes.
	- Los puertos de todos los módulos LAN y SAN que forman parte de la solución, deberán estar licenciados en su totalidad.
	- Los módulos LAN y SAN deberán incluir las licencias de todas sus funcionalidades para todos sus puertos para futuros crecimientos
	- Los módulos de interconectividad deben permitir consolidar los enlaces/comunicaciones de Red externa para mínimo dos chasis adicionales.
	- El módulo de administración debe ser redundante.
	- Debe permitir la administración local y remota de la infraestructura y debe contar con capacidad para:
	o Configuración sencilla y rápida de la infraestructura.
	o Alta disponibilidad y acceso seguro.
	o Brindar seguridad para el módulo de cómputo, la red y los administradores de almacenamiento externo.
	o Mostrar el estado de los dispositivos sin utilizar agente.
Módulo de Administración	- Consola de administración centralizada, que permita ver de manera gráfica el funcionamiento de todos los componentes internos del módulo de cómputo.
	o Se debe poder configurar el hardware y cambiar ajustes del sistema, tales como nivel del RAID, antes del despliegue del sistema operativo.
	o También debe tener la capacidad de capturar los ajustes del hardware y de desplegarlos a través de los módulos de cómputo.
	o Debe tener una funcionalidad KVM virtual en tiempo real y poder realizar un encendido remoto.
	o Alcance a todos los componentes del Chasis y módulos de cómputo.

	o La administración y orquestación unificada deberá soportar hasta 252 módulos de cómputo sin necesidad de incorporar licencias o hardware adicional
	o La solución debe soportar la configuración y automatización de procesos de aprovisionamiento de almacenamiento externo tipo SAN y San Switches.
	- Se deben proveer las licencias de software necesarias para la administración y gestión del Chasis.
	- Se deben proveer dos módulos de cómputo nuevos de la misma marca donde se instalará el software de Gestión Unificada en alta disponibilidad o deberá tenerlo integrado en el chasis como *appliance*.
	- Se debe incluir una licencia perpetua para Gestión Unificada de hardware con la siguiente funcionalidad para DEVOPS:
	o Debe tener un portal web que permita a los usuarios tener la capacidad de administrar y monitorear los componentes de los módulos de cómputo y almacenamiento externo a través de un *dashboard* general.
Gestión Unificada & Licenciamiento	o Debe tener la capacidad de un control de acceso a través de permisos de usuarios e integración con el controlador de dominio existente.
	o Debe tener la capacidad de diseñar perfiles de configuraciones de módulos de cómputo y almacenamiento externo de manera lógica a través de plantillas y ser reutilizables.
	o Debe permitir la actualización de firmware y drivers de los módulos de cómputo de manera automática o manual.
	o Debe permitir visualizar de manera gráfica las conexiones de redes sobre cada módulo de cómputo y sus dependencias de tal manera de ofrecer un mapeo rápido sobre las comunicaciones de los módulos de cómputo.
	o Debe de tener la capacidad de ubicar de manera rápida un módulo de cómputo ya sea por nombre, y/o dirección IP, a través de una búsqueda rápida inteligente.

	o Debe de permitir la integración con otras plataformas de administración de hypervisores tales como VMware y Hyper-V, de tal manera de tener la opción de ejecutar operaciones desde la consola del hypervisor.
	o Debe de poseer integración nativa a través de APIs estándares tipo RESTful.
	o Debe de tener la capacidad de monitorear el consumo de energía de los módulos de cómputo y almacenamiento externo de manera centralizada de tal manera de poder evaluar la carga de energía de cada componente, a su vez la redundancia sobre cada PDU.
	o Debe de tener la capacidad de presentar de manera gráfica el consumo de energía de los componentes de la solución de infraestructura para virtualización.
	- Contar con una plataforma de análisis predictivo que brinde inteligencia con capacidad de predecir y prevenir problemas de infraestructura antes de que sucedan, a través de herramientas de predicción inteligentes como machine learning y/o inteligencia artificial.
	- Análisis del equipo conectada globalmente y utilizar estos datos para predecir y evitar problemas.
Gestión Automatizada	- La plataforma deberá entregar recomendaciones preventivas para reducir las conjeturas sobre la administración de la infraestructura y la confiabilidad de la aplicación
	- Contar con la capacidad de resolver problemas de rendimiento e identificar la causa raíz de los problemas entre el host, las máquinas virtuales (VM) y el almacenamiento externo. También proporciona visibilidad para ubicar máquinas virtuales de "vecinos ruidosos".
	- La implementación deberá incluir la Instalación y configuración de lo siguiente:
Servicios Especializados para la implementación del hardware ofertado	o Instalar físicamente los chasis Blades ofertados en rack incluido en la oferta.
	o Configurar y actualizar el firmware de los chasis Blades ofertados para el CDP.
	o Incluir todas las configuraciones necesarias para la conexión LAN y SAN con la infraestructura existente en el Centro de Datos Principal.

- Adquisición de 2 Servidores Tipo I para gestión

Tabla 44 Especificaciones técnicas de 2 Servidores Tipo 1 para gestión

ESPECIFICACIÓN	REQUERIMIENTO MANDATORIO
Cantidad	2 (dos)
Marca	- Indicar. Ciento por ciento 100% compatible con la infraestructura procesamiento de cómputo de propiedad del Ministerio de Finanzas
Modelo	- Indicar.
Año de Fabricación	- >=2022
Procedencia	- Nuevo de fábrica. No se aceptarán equipos remanufacturados.
Procesamiento	- >= 2 CPUs Intel Xeon de 3ra Generación con al >= 16 cores a 2.6GHz y 48MB de Cache L3
Memoria	- >=1TB DDR4 al menos 3200Mhz con capacidad de crecimiento de al menos 4TB por procesador, cada DIMM debe ser >= 64 GB, con mecanismos de tolerancia rápida de fallas que permitan detectar y corregir errores de memoria antes estos impacten en el sistema.
Slots Expansión	- >=3 slots de expansión para interfaces NIC, HBA, SAS
Discos	- >= 2 Discos 480GB SSD en RAID 1 con una controladora de discos
Interfaces LAN	- >= 2 Puertos físicos de 25/50Gbps
Interfaces SAN	- >= 2 Puertos Fiber Channel de 32Gbps
Seguridad	- Los servidores deberán contar con elementos de protección contra ataques de ransomware embebidos en el Hardware, de tal manera que prevenga y/o detenga la intrusión de código malicioso en los nodos, incluso antes del arranque del hipervisor/sistema operativo, estos mecanismos deberá contar con elementos de recuperación de firmware a un estado saludable en caso de presentarse un escenario de intrusión avanzado.
Servicios Especializados para la implementación del hardware ofertado	- La implementación deberá incluir la Instalación y configuración de lo siguiente:
	o Instalar físicamente los servidores ofertados en las bahías de los chasis ofertados.
	o Configurar y actualizar el firmware de los servidores Blade ofertados.
	o Instalar, configurar y actualizar el sistema operativo de los servidores Blade ofertados.

- Adquisición de 6 Servidores Tipo II para Fabric

Tabla 45 Especificaciones técnicas 6 servidores Tipo II para Fabric

ESPECIFICACIÓN	REQUERIMIENTO MANDATORIO
Cantidad	- 6 (seis)
Marca	- Indicar. Ciento por ciento 100% compatible con la infraestructura procesamiento de cómputo de propiedad del Ministerio de Finanzas
Modelo	- Indicar.
Año de Fabricación	- >=2022
Procedencia	- Nuevo de fábrica. No se aceptarán equipos remanufacturados.
Procesamiento	- >= 2 CPUs Intel Xeon de 3ra Generación con al >= 32 cores a 2.6GHz y 48MB de Cache L3
Memoria	- >=2TB DDR4 al menos 3200Mhz con capacidad de crecimiento de al menos 4TB por procesador, cada DIMM debe ser >=128GB, con mecanismos de tolerancia rápida de fallas que permitan detectar y corregir errores de memoria antes estos impacten en el sistema.
Slots Expansión	- >=3 slots de expansión para interfaces NIC, HBA, SAS
Discos	- >= 2 Discos 480GB SSD en RAID 1 con una controladora de discos
Interfaces LAN	- >= 2 Puertos físicos de 25/50Gbps
Interfaces SAN	- >= 2 Puertos Fiber Channel de 32Gbps
Seguridad	- Los servidores deberán contar con elementos de protección contra ataques de ransomware embebidos en el Hardware, de tal manera que prevenga y/o detenga la intrusión de código malicioso en los nodos, incluso antes del arranque del hipervisor/sistema operativo, estos mecanismos deberá contar con elementos de recuperación de firmware a un estado saludable en caso de presentarse un escenario de intrusión avanzado.
Servicios Especializados para la implementación	- La implementación deberá incluir la Instalación y configuración de lo siguiente: o Instalar físicamente los servidores ofertados en las bahías de los chasis ofertados.

del hardware ofertado	o Configurar y actualizar el firmware de los servidores Blade ofertados.
	o Instalar, configurar y actualizar el sistema operativo de los servidores Blade ofertados.

- Adquisición de 1 Servidor Tipo III para el Directorio Activo

Tabla 46 Especificaciones técnicas 1 Servidor Tipo III para AD

ESPECIFICACIÓN	REQUERIMIENTO MANDATORIO
Cantidad	- 1 (uno).
Marca	- Indicar. Ciento por ciento 100% compatible con la infraestructura procesamiento de cómputo de propiedad del Ministerio de Finanzas
Modelo	- Indicar. El equipo ofertado debe ser el último modelo liberado para la venta por el fabricante y que cumpla con las especificaciones técnicas indicadas.
Año de Fabricación	- >=2022
Procedencia	- Nuevos de fábrica. No se aceptarán equipos remanufactorados.
	-
Tipo	- Rackeable >= 1U
Procesamiento	- >= 2 Sockets Intel Xeon >= 8 cores y >= 2.1GHz
	-
Memoria	- >= 64GB DDR4 >= 2933 Mhz con capacidad de crecimiento de >= 3TB
Slots de Expansión	- >= 3 Slots de expansión para interfaces NIC, HBA, SAS
Discos	- >= 2 Discos de estado sólido de 480GB SAS
Puertos	- >= 2 puertos FC de 16Gbps - >= 2 puertos Ethernet de 10GbE SFP+ - >= 1 puerto Ethernet de 1GbE RJ45 para administración
Fuentes de Poder	- 2 fuentes de poder reduntantes hot plug
Ventilación	- El equipamiento debe contar con todos los ventiladores que soporte el hardware ofertado y deben ser redundantes
Alimentación Eléctrica	- 100-240VAC, 50-60 Hz
Licenciamiento	- Incluir el licenciamiento de Windows Server 2022 Standard.

Seguridad	- El equipo deberá contar con elementos de protección contra ataques de RANSOMWARE embebidos en el Hardware, de tal manera que prevenga y/o detenga la intrusión de código malicioso en los nodos, incluso antes del arranque del sistema operativo, estos mecanismos deberán contar con elementos de recuperación de firmware a un estado saludable en caso de presentarse un escenario de intrusión avanzado.
Servicios Especializados para la implementación del hardware ofertado	- La implementación deberá incluir la Instalación y configuración de al menos lo siguiente: o Instalar física del servidor ofertado en el rack provisto por esta cartera de estado. o Configurar y actualizar el firmware o Instalar, configurar y actualizar el sistema del servidor ofertado. o Incluir todas las configuraciones necesarias para la conexión LAN y SAN con la infraestructura existente en el Centro de Datos Principal

Actividad 1.5 Adquisición de una solución integral de gestión de respaldos para el Ministerio de Economía y Finanzas

La presente contratación comprende la adquisición, implementación, configuración, pruebas, puesta en marcha de la solución gestión de los respaldos para los aplicativos del SINFIP y actualización de las políticas de respaldos.

Para lo cual se requiere:

- Adquirir:
  - 1 Software de gestión de respaldos

Tabla 47 Especificaciones técnicas del software de gestión de respaldos

Especificación	Requerimiento Mandatorio
Capacidad	>=27 (veintisiete terabytes front end)
Marca	Indicar.
Tipo	Indicar.
Versión	Última versión liberada por el fabricante.

Compatibilidad Plataforma MEF	La solución de software de respaldos debe ser compatible con las plataformas de servidores que posee esta Cartera de Estado (Sistemas Operativos con soporte de fabricante/Aplicaciones con soporte de fabricante e Infraestructura detallados en la sección "INFORMACIÓN QUE DISPONE LA ENTIDAD". Incluir certificado del fabricante que permitirá validar lo solicitado.
Compatibilidad componentes ofertados	Todos los componentes de hardware y de software de la solución ofertada deben ser compatibles entre sí. Incluir certificado del fabricante que permitirá validar lo solicitado.
Compatibilidad con Bases de Datos del MEF	La solución de software de respaldos debe ser certificada para las Base de Datos con soporte de fabricante detallados en la sección "INFORMACIÓN QUE DISPONE LA ENTIDAD". Incluir certificado del fabricante que permitirá validar lo solicitado. (Adjuntar documentación técnica de SAP, Microsoft, Oracle / URL del sitio oficial de cada fabricante que permita validar lo solicitado), o certificado de los fabricantes.
Capacidad front end terabyte	>= 27 TB. Debe permitir hacer uso de todos los agentes o características necesarios para la solución sin límite de cantidad, para la totalidad de la capacidad solicitada.
Alta Disponibilidad	La solución de software de respaldos debe ser instalada y configurada en clúster en modalidad Activo – Pasivo. Lo que garantizará la continuidad del servicio de respaldos.
Características	Software de Respaldo Corporativo/Enterprise, que permita la administración centralizada de los respaldos y la generación/copia de los respaldos solicitados por el MEF. Que debe incluir: · Interface gráfica

· El software de respaldo debe permitir la administración centralizada de los respaldos y la generación/copia de los respaldos.
· La consola central debe soportar la instalación en Sistemas operativos Linux (RedHat o SUSE) y/o Windows (2019 o superior).
· Debe gestionar todas las operaciones de respaldo y mantener una base de datos interna que contenga al menos:
· a. Catálogo de todas las operaciones de respaldo.
· b. Clientes a respaldar.
· c. Dispositivos de respaldo.
· d. Las licencias de cada uno de los componentes de la aplicación.
La administración de las licencias y la distribución de los componentes (agentes) deberá ser gestionada de forma centralizada desde la consola y las mismas deberán ser instaladas en los servidores de donde se obtendrá la información a ser respaldada.
· Debe tener la capacidad para poder respaldar el catálogo de los respaldos con todos sus componentes para una pronta recuperación en caso de daño o corrupción de la base de datos interna.
· Debe tener la capacidad de manejar control de acceso basado en roles que permita:
· Roles de Seguridad de la solución.
· Administración de Respaldos.
· Administración de cargas específicas de respaldos.
· Debe tener la funcionalidad de realizar respaldos encriptados de la información con el estándar de la industria AES 256 desde el servidor desde donde se encuentran los datos hacia el servidor que realiza la escritura en los dispositivos de respaldo.

· Debe tener la capacidad de respaldar servidores en forma ilimitada sin incorporar licencias o suscripciones para la capacidad de licenciamiento (27TB).

· Debe poder respaldar al menos servidores de plataformas con sistema operativo Windows Server, Linux Red Hat Enterprise, SUSE Linux Enterprise for SAP, HP-UX.

· Debe tener la capacidad de generar respaldos a través de la red LAN

· Deberá tener la capacidad de generar respaldos a través de la red SAN sin utilización de la red LAN.

· Deberá tener la capacidad de generar respaldos al almacenamiento de disco y a cinta magnética de respaldo como mínimo.

· Deberá tener la capacidad de generar copias de respaldo a diferentes medios de almacenamiento de forma simultánea con el respaldo principal o bien diferido en el tiempo.

· El software de respaldos debe tener la capacidad de generar respaldos a los almacenamientos de corta y larga retención, y a la librería de cintas magnéticas de respaldo solicitadas, utilizando exclusivamente los elementos de su arquitectura como roles/proxys/servidor de medios o equipamiento adicional los cuales deben ser de la propia marca del fabricante del software y hardware ofertado.

· Debe contar con asistentes (Wizards) y plantillas estándar para configurar las operaciones de respaldo.

· Debe poder realizar respaldos en línea tanto de archivos abiertos como de aplicaciones.

· Debe poseer la capacidad de integrarse y realizar backups en caliente de las principales bases de datos de mercado, como son Oracle, MS SQL Server, MySQL, SAP Hana

· El software de respaldos debe integrarse tanto con servidores físicos como virtuales para el respaldo de las plataformas detalladas en punto Información que dispone la entidad y realizar el respaldo de los archivos de control de transacciones, sin interrupción del servicio.

· Debe poseer la capacidad de realizar backups en caliente de aplicaciones tales como Sharepoint, SAP, SAP HANA 2.0 SPS 03, sin interrupción del servicio.

· Deberá tener la capacidad de integrarse con ambientes virtuales Hyper-V, VMWARE y poder realizar respaldos en línea en su entorno de virtualización, sin interrupción del servicio.

· El software de respaldos debe tener la capacidad de generar reportes para visualizar el estado de los jobs y los clientes de respaldo

· Deberá poder generar al menos los siguientes tipos de respaldos:

· Completos (full backup) en disco

· Incrementales de tal forma que se pueda constituir un respaldo completo (full) con un mínimo de espacio en disco sin tener que replicar la información que no ha sido cambiada desde el primer respaldo completo (full).

· Deberá proveer facilidades de Disaster Recovery para los servidores físicos y virtuales respaldados con sistemas operativos Microsoft Windows Server y Linux Red Hat Enterprise, SUSE Linux Enterprise for SAP sin costo adicional.

· Debe poseer mecanismos de deduplicación en el origen y destino y la capacidad de generar repositorios de deduplicación sin agregar software adicional.
· Debe tener la capacidad de replicar el catálogo de la operación de respaldo del Centro de Datos Principal al Centro de Datos Alterno y viceversa.
· Debe tener la capacidad de generar/copiar los respaldos del Centro de Datos Principal al Centro de Datos Alterno.
· La solución debe incluir Inteligencia Artificial con Machine Learning o tecnologías similares; que establezca patrones de comportamiento de los respaldos y detecte anomalías o cambios bruscos en las políticas definidas, basados en cuatro puntos:
· Tamaño de los datos respaldados.
· Cantidad de archivos respaldados.
· Factor de deduplicación del respaldo. y,
· Tiempos de los respaldos
· La solución debe incluir “Malware Scan” o tecnologías similares, ya sea con una herramienta incluida con el licenciamiento propuesto o integrable con la solución de antivirus/antimalware que dispone el MEF, con las políticas de respaldo de data no estructurada Tipo Estándar (Unix/Linux/NFS) o Windows (CIFS/SMB), de manera que pueda, realizar un chequeo posterior a la ejecución del respaldo o previo a la recuperación, generando el borrado del respaldo y su contenido, frente a la detección positiva de alguna traza de antivirus o Ransomware.
· La solución debe incluir dentro del licenciamiento un esquema de replicación para ambientes virtuales VMware y Hyper-V para propósito de Recuperación de Desastres DR.
· Los servicios de replicación de respaldos desde el Centro de Datos Principal hacia el Centro de Datos Alterno o viceversa deben ser gestionados por el software de respaldo ofertado y utilizando las características de

compresión y deduplicación de los sistemas de los almacenamientos de corta y larga retención del Centro de Datos Principal y Centro de Datos Alterno.

- 2 almacenamientos de corta retención para el Centro de Datos Principal y para el Centro de Datos Alterno

Tabla 48 Especificaciones técnicas 2 almacenamiento de corta retención

Especificación	Requerimiento Mandatorio
Cantidad	>= 2. Uno (1) para CDP y uno (1) para CDA.
Marca	Indicar. Compatible con la actual infraestructura propiedad del Ministerio de Finanzas a nivel de protocolos estándares de la industria.
Modelo	Indicar. El equipo ofertado debe ser el último modelo liberado para la venta por el fabricante a la fecha de presentación de la oferta y que cumpla con las especificaciones técnicas indicadas.
Año de Fabricación	>= 2022
Procedencia	Nuevos de fábrica. No se aceptarán equipos re-manufacturados.
Instalación	Instalación Física en el CDP.
	Los equipos serán instalados en el Centro de Datos del Ministerio de Economía y Finanzas en el rack estándar de 42U incluido en la solución ofertada.
	Para la ciudad de Guayaquil en MEF proveerá el espacio en el rack. El Proveedor deberá indicar la cantidad de espacio necesario para la instalación de su equipo, para la ciudad de Guayaquil la solución ofertada deberá incluir los accesorios necesarios de montaje y anclaje para su instalación, los cuales deberán ser provistos por el oferente.
Características de cada almacenamiento	
Capacidad requerida	>= 70 TiB usable en tecnología RAID 6 o tecnología similar por equipo, luego de aplicado el Raid.

	Los almacenamientos ofertados deben tener RAID 1 o RAID 10 o tecnología similar para el sistema operativo y RAID 6 o tecnología similar para los datos de Backup con disco HotSpare dedicado
Capacidad escalable	El equipo ofertado debe permitir escalabilidad modular >= 400 TiB
Memoria RAM	El equipo ofertado debe incluir >= 256Gb RAM
CPU	El equipo ofertado debe incluir >=16 cores Intel ó AMD >=2.2 Ghz
Tecnología de Discos Soportadas	Unidades de discos SAS de 7200 RPM y capacidad >= 8 TB
Protección de Datos	En caso de un fallo de la energía, la solución ofertada deberá evitar cualquier pérdida de datos teniendo en cuenta el esquema de protección de raid o tecnología similar a nivel de hardware y la protección de los datos en los volúmenes bajo esquema de "Journaling" a nivel del manejador de los volúmenes.
Protocolos Soportados	Debe cumplir al menos: CIFS o NFS
Interfaces de comunicación	>= 2 puertos Ethernet RJ45 >= 1 Gbps. >= 4 puertos Ethernet >= 10/25 Gbps SFP. >= 4 puertos de fibra canal >= 16 Gbps**.**
Fuente de poder	Redundantes para tolerancia a fallas, se debe entregar con todas las fuentes de poder que soporte el hardware ofertado.
Ventilación	El equipamiento debe contar con todos los ventiladores que soporte el hardware ofertado y deben ser redundantes.
Funcionalidades	El hardware ofertado deberá incluir en la oferta la licencia de deduplicación sin costo adicional para la capacidad ofertada del almacenamiento. Los almacenamientos de corta y larga retención ofertados deben permitir la replicación de información desde los almacenamientos ofertados para el Centro de Datos Principal hacia los almacenamientos ofertados para el Centro de Datos Alterno o viceversa, la replicación deberá ser

parametrizable en cuanto al ancho de banda que utilizará para la replicación.
Al utilizar deduplicación, la réplica de información desde el Centro de Datos Principal de la ciudad de Quito hacia el Centro de Datos Alterno de la ciudad de Guayaquil será solo de información a nivel de bloques que no esté (diferencial) en el almacenamiento destino.
Copia de seguridad basado en disco
Cifrado AES de 256 bits integrado.
El almacenamiento debe tener inmutabilidad para la capacidad total contratada.
Los almacenamientos ofertados deben brindar inmutabilidad de los respaldos de manera que se pueda establecer un esquema WORM (Write Only, Read Many) para las copias de seguridad almacenadas bajo un período de tiempo establecido que puede ser permanente.
En cuanto a Inmutabilidad, los almacenamientos ofertados deben garantizar el cumplimiento de lo establecido por las normas internacionales SEC Rule 17a-4f, FINRA Rule 45511©.
En el manejo de inmutabilidad, los almacenamientos ofertados no deben estar ligados al reloj del sistema operativo, esto con el fin de evitar posibles alteraciones que puedan afectar los respaldos almacenados bajo esta característica, u ofrecer un esquema que cumpla lo solicitado adicionando los componentes de hardware y software necesarios.
Los almacenamientos ofertados deben incluir un sistema de detección y prevención de intrusos IDS /IPS directamente de fábrica sin requerir licenciamiento adicional, en el caso de no tenerlo incluir los elementos de hardware y software necesarios a fin de cumplir lo requerido.
Los almacenamientos ofertados deben incluir >=2 capas de seguridad de acceso para evitar que algún servicio externo pueda lograr acceso directo a los sistemas de archivos del almacenamiento.
La solución ofertada debe permitir la automatización de procesos de recuperación de desastres de un servidor, de una aplicación, servicio o proceso de negocio, esto a través de la recuperación a partir de los respaldos, o apoyado en procesos de replicación complementarios, logrando tener diferentes niveles de recuperación de los servicios.
La solución debe incluir la capacidad de automatizar la recuperación en un sitio diferente en caso de desastre, donde el sitio remoto puede ser un datacenter on premise.

Monitoreo	Debe incluir el monitoreo proactivo de componentes por parte del fabricante del hardware ofertado.
Herramienta de administración	Incluir una herramienta basada en web para administrar el almacenamiento de corta y larga retención ofertado.
Alimentación eléctrica para el CDP	Redundante, 200 a 240 VAC, 50 a 60 Hz.

- 2 almacenamientos de larga retención de respaldos a disco para el Centro de Datos Principal y para el Centro de Datos Alterno

Tabla 49 Especificaciones técnicas 2 almacenamiento de larga retención

Especificación	Requerimiento Mandatorio
Cantidad	>=2. Uno (1) para CDP y uno (1) para CDA.
Marca	Indicar. Compatible con la actual infraestructura propiedad del Ministerio de Finanzas a nivel de protocolos estándares de la industria.
Modelo	Indicar. El equipo ofertado debe ser el último modelo liberado para la venta por el fabricante a la fecha de presentación de la oferta y que cumpla con las especificaciones técnicas indicadas.
Año de Fabricación	>= 2022
Procedencia	Nuevos de fábrica. No se aceptarán equipos re-manufacturados.
Requerimientos por cada almacenamiento	
Cantidad de Controladoras de discos	>= 2 en modalidad activo – pasivo, por cada almacenamiento**.**
Características de las controladoras	Debe asegurar la disponibilidad de servicio, durante:

	- Tareas de mantenimiento
	- Actualización de microcódigo, componentes.
	- Actualización de parches.
	- Cambio de partes y piezas.
	Arquitectura de procesamiento totalmente distribuida, paralela y tolerante a fallos.
Capacidad requerida	>= 600 TiB usable en tecnología RAID 6 o tecnología similar por cada almacenamiento.
Capacidad escalable	El equipo ofertado debe permitir escalabilidad modular
	>= 2.0 PB usable luego de aplicado el RAID o tecnología similar por cada almacenamiento
Memoria RAM por controladora	>= 384Gb RAM (paletas de 32 GB) con capacidad de crecimiento de >=1 TB por almacenamiento.
CPU por controladora	El equipo ofertado debe incluir Dual Intel® Xeon® Scalable Processors con >=10 cores por procesador Intel >=2.0 GHz
	La arquitectura de procesamiento totalmente distribuida, paralela y tolerante a fallos.
Instalación	Instalación Física en el CDP.
	Los equipos serán instalados en el Centro de Datos del Ministerio de Economía y Finanzas en el rack estándar de 42U incluido en la solución ofertada.
	La solución ofertada deberá incluir los cables de red y accesorios necesarios para su instalación y montaje, los cuales deberán ser provistos por el oferente

	Para la ciudad de Guayaquil la solución ofertada deberá incluir los accesorios de anclaje y montaje necesarios para su instalación.
Funcionalidades	Copia de seguridad basado en disco
	Los almacenamientos ofertados deben integrarse con la solución de software de gestión de respaldo ofertada para la retención y protección de datos (información de respaldos) a largo plazo de manera consistente.
	Los almacenamientos ofertados deben incluir en la oferta la licencia de deduplicación sin costo adicional para la capacidad total del almacenamiento ofertada.
	Los almacenamientos ofertados deben permitir la replicación de información desde los almacenamientos ofertados para el Centro de Datos Principal (corta y larga retención) hacia los almacenamientos ofertados para el Centro de Datos Alterno o viceversa, la replicación deberá ser parametrizables en cuanto al ancho de banda que utilizará para este proceso.
	Al utilizar deduplicación, la réplica de información desde el Centro de Datos Principal de la ciudad de Quito hacia el Centro de Datos Alterno de la ciudad de Guayaquil será solo de información a nivel de bloques que no esté (diferencial) en el almacenamiento destino.
	Cifrado AES de 256 bits integrado.
	Los almacenamientos de larga retención ofertados deben contar inmutabilidad de las imágenes de respaldo lo que permitirá bloquear el dispositivo y no permitir ninguna operación que pueda conducir a la destrucción de datos.
	Los almacenamientos de larga retención ofertados deben contar IDS (Intrussion Detection System) / IPS (Intrussion Prevention System), directamente de fábrica sin requerir licenciamiento adicional, en el caso de no tenerlo incluir los elementos de hardware y software necesarios a fin de cumplir lo requerido
Tecnología de Discos Soportadas	Unidades de discos SAS de >= 7200 RPM y capacidad >= 10 TB
Protección de Datos	En caso de un fallo de la energía, la solución ofertada deberá evitar cualquier pérdida de datos.
Protocolos Soportados	Debe cumplir al menos:
	CIFS/NFS o MSDP

Interfaces de comunicación por cada almacenamiento	>= 4 puertos Ethernet RJ45 >= 1 Gbps
	>= 4 puertos Ethernet >= 10 Gbps SFP
	En caso de requerir puertos adicionales, el oferente deberá incluir un switch de 10Gbps SFP con los puertos que sean necesarios.
Fuente de poder	Redundantes para tolerancia a fallas, se debe entregar con todas las fuentes de poder que soporte el hardware ofertado.
Ventilación	El equipamiento debe contar con todos los ventiladores que soporte el hardware ofertado y deben ser redundantes.
Monitoreo	Debe incluir el monitoreo proactivo de componentes por parte del fabricante del hardware ofertado.
Herramienta de administración	Incluir una herramienta basada en web para administrar la solución ofertada.
Alimentación eléctrica para el CDP	Redundante, 200 a 240 VAC, 50 a 60 Hz.

- 2 servidores donde se instalará el software para la gestión de los respaldos

Tabla 50 Especificaciones técnicas 2 servidores

Especificación	Requerimiento Mandatorio
Cantidad	>=2
Marca	Indicar. Compatible con la actual infraestructura propiedad del Ministerio de Finanzas a nivel de protocolos estándares de la industria.
Modelo	Indicar. El equipo ofertado debe ser el último modelo liberado para la venta por el fabricante a la fecha de presentación de la oferta y que cumpla con las especificaciones técnicas indicadas.
Año de Fabricación	>= 2022
Procedencia	Nuevos de fábrica. No se aceptarán equipos re-manufacturados.
Tipo	Rackeable >= 2 U por cada servidor
Características de cada servidor	
Procesamiento	>= 2 sockets Intel Xeon-Gold >= 8 cores y >= 3,6 Ghz

Memoria	>=128 GB DDR4 >= 3200 Mhz con capacidad de crecimiento de >=1.0 TB (Incluir DIMMS de >=32GB)
Slots Expansión	>=6 slots de expansión para interfaces NIC, HBA, SAS
Discos	>= 4 Discos 1.2TB SAS 10K
Puertos	>= 2 puertos FC SFP+ >= 16 Gbps
	>= 2 puertos FC SFP+ >= 10 Gbps
	>= 1 puerto Ethernet RJ54 >= 1 Gbps para administración.
Fuente de poder	Redundantes para tolerancia a fallas, se debe entregar con todas las fuentes de poder que soporte el hardware ofertado.
Seguridad	El equipo deberá contar con elementos de protección contra ataques de RANSOMWARE embebidos en el Hardware, de tal manera que prevenga y/o detenga la intrusión de código malicioso en los nodos, incluso antes del arranque del sistema operativo, estos mecanismos deberán contar con elementos de recuperación de firmware a un estado saludable en caso de presentarse un escenario de intrusión avanzado.
Ventilación	El equipamiento debe contar con todos los ventiladores que soporte el hardware ofertado y deben ser redundantes.
Alimentación eléctrica	Redundante, 200 a 240 VAC, 50 a 60 Hz.
Instalación	Instalación Física en el CDP.
	Los equipos serán instalados en el Centro de Datos del Ministerio de Economía y Finanzas en el rack estándar de 42U incluido en la solución ofertada.

- 1 librería robótica de cintas

Tabla 51 Especificaciones técnicas 1 librería robótica

Especificación	Requerimiento Mandatorio
Cantidad	>=1
Marca	Indicar. Compatible con la actual infraestructura propiedad del Ministerio de Finanzas a nivel de protocolos estándares de la industria
Modelo	Indicar. El equipo ofertado debe ser el último modelo liberado para la venta por el fabricante a la fecha de presentación de la oferta y que cumpla con las especificaciones técnicas indicadas.
Año de Fabricación	>= 2022
Procedencia	Nuevos de fábrica. No se aceptarán equipos remanufacturados.
Tipo	Rackeable
Características	Interface de panel frontal tipo GUI
	Conectividad de fibra nativa a la Red SAN, con interfaz tipo FC.

	>= 5 mail slots para magazine
	Librería con capacidad de particionamiento y flexibilidad para cada unidad ofrecida. La licencia requerida para la partición debe ser incluida.
Drives instalados	>= 3 unidas de cinta FC LTO Gen-9.
Puertos	>= 2 puertos de fibra canal >= 8 Gbps (por cada drive instalado)
	>= 1 puerto Ethernet RJ45 >= 1 Gbps para administración.
Slots	>= 40 ranuras para cartucho.
	>= 1 lector de código de barras.
Estándares	Debe cumplir con el estándar INCITS / T10 SCSI-3 como mínimo.
Fuentes de poder	Redundantes para tolerancia a fallas, se debe entregar con todas las fuentes de poder que soporte el hardware ofertado.
Ventilación	El equipamiento debe contar con todos los ventiladores que soporte el hardware ofertado y deben ser redundantes.
Alimentación eléctrica	Redundante, 200 a 240 VAC, 50 a 60 Hz.
	El oferente debe incluir unidades de distribución de energía (PDUs) para la cantidad de corriente que consumirá la solución a 220 voltios, dividido en circuitos independientes, cada uno con interruptores de corriente (breakers) de protección.
Suministros.	100 cintas LTO – 9 y 100 etiquetas con el siguiente formato de código de barras: MFM700 AL MFM799.
	- 2 cintas de limpieza para drives instalados.

5.1.2.1 Componente 2: Reducción la brecha tecnológica y operativa del MEF (Software)

Actividad 2.1 Consultoría para la actualización de la Nube Privada

El presente proyecto tiene por finalidad la actualización tecnológica de la versión y funcionalidad del software de Nube Privada propiedad de esta Cartera de Estado mediante la implementación, configuración, pruebas y puesta en marcha de:

- Clúster de Gestión conformado por dos servidores Blade que se utilizará para la gestión de la Nube Privada
- Clúster de Gestión conformado por seis servidores Blade que se utilizará para alojar todo el ambiente productivo de los servicios y aplicaciones del SINFIP.

Las características que deben considerarse en la implementación corresponden a:

- Diseño Lógico
- Descripción Componentes funcionales de Nube Privada.
- Roles de Servidor de Gestión, Fábrica (Hosts), Virtuales(Invitados)

- Descripción de la configuración de Lógica Networks, Virtual Machine Networks y Virtual Switches de acuerdo a las nuevas funcionalidades de System Center.
- Descripción de las configuraciones de los clústeres de Gestión y Producción
- Instalación de las siguientes máquinas virtuales:
  - Virtual Machine Manager.
  - Bases de Datos del Management en configuración Clúster de dos nodos virtuales de MS SQL Server.
  - Validación de las configuraciones.

La implementación debe realizarse con el mínimo impacto al ambiente productivo, manteniendo la disponibilidad y continuidad de todos los servicios y corresponde a:

- Configuración de los Host Físicos
- Creación del clúster de administración de la plataforma. (Gestión).
- Creación del clúster de producción de la plataforma. (Producción).
- Migración de servidores virtuales.
- Ejecución de Pruebas funcionales.
- Creación de 3 plantillas de máquinas virtuales.
- Memorias Técnicas.
- Transferencia de conocimiento.

5.2 Viabilidad Financiera fiscal

Para el desarrollo de la viabilidad financiera fiscal se han desarrollado los siguientes aspectos:

5.2.1 Metodologías utilizadas para el cálculo de la inversión total, costos de operación y mantenimiento, ingresos y beneficios

Para el cálculo de la inversión total se realizó reuniones de trabajo con fabricantes-proveedores de equipamiento de infraestructura especializado a nivel internacional para cada una de las futuras contrataciones; utilizando como base las cotizaciones con especificaciones técnicas y precios se calcularon los costos referenciales promedio para el presente proyecto.

Los costos de mantenimiento por normativa legal, están incluidos en las cotizaciones proporcionadas por los fabricantes del equipamiento de infraestructura.

Para la reducción de la brecha tecnológica se han obtenido cotizaciones de proveedores especializados en consultoría e implementación de la actualización de la versión de la Nube Privada.

5.2.2 Identificación y valoración de la inversión total, costos de operación y mantenimiento, ingresos y beneficios

5.2.2.1 Inversión Total

Una vez analizadas las cotizaciones y especificaciones técnicas de los fabricantes se han determinado los siguientes valores para el 2023 y 2024 utilizando, el promedio de valores de las cotizaciones recibidas:

Tabla 52 Inversión total por componentes y actividades

COMPONENTE	ACTIVIDAD	TIPO DE INTERV.	ITEM PRESUP.	2023					2024					TOTAL INVERSIÓN US
				COSTO UNITARIO (SIN IVA) US	CANT.	SUBTOTAL US (SIN IVA)	IVA US	TOTAL	COSTO UNITARIO US (SIN IVA)	CANT.	SUBTOTAL US (SIN IVA)	IVA US	TOTAL	
C1: Fortalecimiento de la infraestructura tecnológica del SINFIP (Hardware)	A.1.1 Fortalecimiento de los equipos balanceadores de enlaces, DNS y aplicaciones para el Centro de Datos Principal del Ministerio de	Infraestructura	840107	689.562,24	1	689.562,24	82.747,47	772.309,71	295.526,68	1	295.526,68	35.463,20	330.989,88	**1.103.299,59**
	A.1.2 Fortalecimiento de los equipos de seguridad firewall perimetral y firewall IPS de Data Center para el Centro de Datos Principal	Infraestructura	840107	641.442,90	1	641.442,90	76.973,15	718.416,05	274.904,10	1	274.904,10	32.988,49	307.892,59	**1.026.308,64**
	A.1.3 Adquisición de Infraestructura para el reforzamiento de conectividad LAN del Centro de Datos Principal del	Infraestructura	840107	431.305,65	1	431.305,65	51.756,68	483.062,33	184.845,28	1	184.845,28	22.181,43	207.026,71	**690.089,04**
	A.1.4 Adquisición de Infraestructura y Servicio para el reforzamiento de la nube privada	Infraestructura	840107	1.558.312,88	1	1.558.312,88	186.997,55	1.745.310,43	-	1	-	-	-	**1.745.310,43**
	A.1.5 Adquisición de una solución integral de gestión de respaldos para el Ministerio de Economía y Finanzas	Infraestructura	840107	1.282.457,59	1	1.282.457,59	153.894,91	1.436.352,50	549.624,68	1	549.624,68	65.954,96	615.579,64	**2.051.932,14**
C 2: Reducción de la brecha tecnológica y operativa del MEF (Software)	A.2.1 Consultoría e implementación de la actualización de la versión de la Nube Privada	Consultoría	730601	6.000,00	1	6.000,00	720,00	6.720,00	54.000,00	1	54.000,00	6.480,00	60.480,00	**67.200,00**
			Total	**4.609.081,26**		**4.609.081,26**	**553.089,75**	**5.162.171,02**	**1.358.900,74**		**1.358.900,74**	**163.068,09**	**1.521.968,82**	**6.684.139,84**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo de gestión del proyecto

5.2.2.2 Costos de operación y mantenimiento

El proyecto no contempla costos de costos de operación y mantenimiento, ya que como se mencionó en el numeral 5.2.1 por normativa legal, están incluidos en los montos de los contratos, así como el costo de instalación y soporte de equipos.

5.2.2.3 Ingresos

El proyecto del Ministerio de Economía y Finanzas no genera ingresos por el concepto de servicios relacionados con la actualización de la infraestructura tecnológica.

5.2.2.4 Vida útil

Para el cálculo de los flujos económicos y financieros se considera una vida útil del proyecto de 5 años, con lo cual se mantendrá la disponibilidad y continuidad de las aplicaciones y servicios tecnológicos del Sistema Nacional de las Finanzas Públicas, SINFIP, en una plataforma tecnológica actualizada, segura y confiable.

5.2.3 Flujo financiero fiscal

A continuación, se expresa el siguiente flujo financiero del proyecto.

Tabla 53 Flujo financiero fiscal

Período	Año 0	Año 1
	2023	2024
INGRESOS (US Corrientes) (a)	**-**	**-**
EGRESOS (b)	**5.162.171,02**	**1.521.968,82**
INVERSIÓN (US)	5.162.171,02	1.521.968,82
Costos US	5.162.171,02	1.521.968,82
A.1.1 Fortalecimiento de los equipos balanceadores de enlaces, DNS y aplicaciones para el Centro de Datos Principal del Ministerio de Economía y Finanzas	772.309,71	330.989,88
A.1.2 Fortalecimiento de los equipos de seguridad firewall perimetral y firewall IPS de Data Center para el Centro de Datos Principal	718.416,05	307.892,59
A.1.3 Adquisición de Infraestructura para el reforzamiento de conectividad LAN del Centro de Datos Principal del Ministerio de Economía y Finanzas	483.062,33	207.026,71
A.1.4 Adquisición de Infraestructura y Servicio para el reforzamiento de la nube privada	1.745.310,43	-
A.1.5 Adquisición de una solución integral de gestión de respaldos para el Ministerio de Economía y Finanzas	1.436.352,50	615.579,64
A.2.1 Consultoría e implementación de la actualización de la versión de la Nube Privada	6.720,00	60.480,00
FLUJO DE CAJA (a-b) US	**-5.162.171,02**	**1.521.968,82**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo de gestión del proyecto

5.2.4 Indicadores financieros fiscales

Para la evaluación financiera se ha considerado los siguientes indicadores financieros:

Tabla 54 Indicadores financieros

Parámetros de evaluación financiera	Valores
Tasa de descuento (TD)	12%
Valor Actual Neto (VAN)	-6.521.071,75
Tasa interna de retomo (TIR)	#¡NUM!
Relación beneficio costo (B/C)	-

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo de gestión del proyecto

Es preciso aclarar que el proyecto no genera ingresos, por lo tanto, el VAN es negativo, la TIR y la relación B/C no es posible calcular, tal y como se visualiza en la tabla de indicadores financieros, generando error en el resultado.

5.3 Viabilidad Económica

Para el desarrollo de la viabilidad económica fiscal se han desarrollado los siguientes aspectos:

5.3.1 Metodologías utilizadas para el cálculo de la inversión total, costos de operación y mantenimiento, ingresos y beneficios.

Para el cálculo de la inversión total, costos de operación y mantenimiento ingresos se expresa en el numeral 5.2.2.

Considerando el problema del proyecto "*elevado riesgo en la prestación de servicios institucionales del MEF a las entidades del sector público por la desactualización de la infraestructura tecnológica*". Los beneficios están reflejados en los ahorros generados para el periodo de 2023-2027.

Para la identificación y cálculo de los Costos evitados por **no uso** de los sistemas tecnológicos **- el tiempo ocioso por no disponer los sistemas tecnológicos en relación con la remuneración promedio de los usuarios que constituyen la demanda efectiva -** en caso de falla de la estructura tecnológica, en este sentido y con el fin de calcular los costos evitados han consideraron los siguientes aspectos: probabilidad de falla, impacto en los servicios tecnológicos, brecha promedio de reducción del riesgo, porcentaje de incidencia de no contar con infraestructura, sueldo promedio de usuarios de sistemas tecnológicos,

usuarios de sistemas tecnológicos y porcentaje de incidencia por no uso de sistemas tecnológicos por falla de infraestructura tecnológica.

- **Probabilidad** de falla de funcionamiento de infraestructura tecnológica.

Tabla 55 Probabilidad de falla

Denominación	Situación actual				
	2018	2019	2020	2021	2022
Nube	80%	80%	80%	80%	80%
Sistema respaldo	80%	80%	80%	80%	80%
Balanceador	35%	50%	65%	80%	80%
Switch	45%	60%	75%	80%	80%
Firewall	20%	50%	60%	60%	60%
Promedio	**52%**	**64%**	**72%**	**76%**	**76%**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo de gestión del proyecto

Una vez analizada la información técnica e histórica de la Subsecretaría de Innovación de las Finanzas Públicas, se ha identificado que para el año 2022 existe una probabilidad de falla del 76%, debido a la obsolescencia de una parte de la infraestructura tecnológica.

- **Impacto** en el funcionamiento de infraestructura tecnológica.

Tabla 56 Impacto en el funcionamiento

Denominación	Situación actual				
	2018	2019	2020	2021	2022
Nube	100	100	100	100	100
Sistema respaldo	80	80	80	80	80
Balanceador	80	80	80	80	80
Switch	100	100	100	100	100
Firewall	100	100	100	100	100
Promedio	**92**	**92**	**92**	**92**	**92**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo de gestión del proyecto

Se ha identificado para el año 2022 un valor de 92 puntos de impacto en el caso de fallas de equipos de infraestructura tecnológica.

- **Riesgo** en la prestación de servicios institucionales del MEF a las entidades del sector público por la desactualización de la infraestructura tecnológica.

Tabla 57 Riesgo en la prestación de servicios (situación actual)

Denominación	Situación actual				
	2018	2019	2020	2021	2022
Nube	80%	80%	80%	80%	80%
Sistema respaldo	64%	64%	64%	64%	64%
Balanceador	28%	40%	52%	64%	64%
Switch	45%	60%	75%	80%	80%
Firewall	20%	50%	60%	60%	60%
Promedio	**47%**	**59%**	**66%**	**70%**	**70%**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo de gestión del proyecto

Se ha identificado para el año 2022 un elevado riesgo del 70% en la prestación de servicios institucionales del MEF a las entidades del sector público por la obsolescencia de la infraestructura tecnológica.

Tabla 58 Proyección del Riesgo en la prestación de servicios (situación deseada)

Denominación	Situación deseada				
	2023	2024	2025	2026	2027
Nube	10%	25%	40%	60%	80%
Sistema respaldo	10%	22%	34%	50%	64%
Balanceador	10%	22%	34%	50%	64%
Switch	10%	25%	40%	60%	80%
Firewall	10%	25%	40%	60%	60%
Promedio	**10%**	**24%**	**38%**	**56%**	**70%**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo de gestión del proyecto

Para el año 2023, una vez actualizada la infraestructura tecnológica el riesgo de falla es del 10%, mismo que se va incrementado en el transcurso de la vida útil del proyecto, hasta alcanzar el 70% en el año 2027.

- Brecha de riesgo de funcionamiento de infraestructura tecnológica.

Tabla 59 Brecha de riesgo de funcionamiento

Denominación	Brecha (Situación deseada -Situación actual)				
	2023	2024	2025	2026	2027
Nube	-70%	-55%	-40%	-20%	0%
Sistema respaldo	-54%	-42%	-30%	-14%	0%
Balanceador	-54%	-42%	-30%	-14%	0%
Switch	-70%	-55%	-40%	-20%	0%
Firewall	-50%	-35%	-20%	0%	0%
Promedio	**-60%**	**-46%**	**-32%**	**-14%**	**0%**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo de gestión del proyecto

Para el año 2023 una vez actualizada la infraestructura tecnológica, la brecha del riesgo de falla de equipos es del 60%, misma que va disminuyendo en la vida útil del proyecto hasta llegar al 0% en el año 2027.

- Porcentaje de no contar con infraestructura tecnológica actualizada

Tabla 60 Porcentaje deducible de no contar con infraestructura (1+brecha promedio)

Denominación	Valores comparativos				
	2023	2024	2025	2026	2027
Brecha promedio de reducción del riesgo	-60%	-46%	-32%	-14%	0%
Factor deducible de no contar con infraestructura	40%	54%	68%	86%	100%

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo de gestión del proyecto

Se refiere al factor que permite identificar en términos absolutos la afectación, como valor deducible de **no contar con infraestructura**, esto es (1 + brecha promedio). La brecha promedio de calcula tomando en consideración la situación actual comparada con la situación deseada se reduce para el 2023 en un 60%, hasta llegar al 0% en el año 2027; mientras que, el factor de deducible para el cálculo de costos evitados para el 2023 es del 40% y va creciendo hasta el 100% en el año 2027; en ambos casos, debido a que el equipamiento va perdiendo vigencia tecnológica.

- Usuarios directos de sistemas tecnológicos

Tabla 61 Usuarios del PGE de sistemas tecnológicos

Módulo	Número de Usuarios
Contabilidad	1.796
Nomina	1.250
Presupuesto	1.427
Tesorería	1.472
Administración de Usuarios	475
Total	**6.420**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo de gestión del proyecto

El total de usuarios de los sistemas tecnológicos que brinda el Ministerio de Economía y Finanzas del Ecuador de los distintos módulos de los sistemas tecnológicos del SINFIP es de 6.420 usuarios, mismo que forman parte de la totalidad de la demanda efectiva.

- Sueldo promedio de usuarios de sistemas tecnológicos.

Tabla 62 Sueldo promedio de usuarios

Remuneraciones	Número de Usuarios
Total de remuneraciones (USD)	8.553.479
Número de usuarios (servidores)	6.420
Remuneración promedio (servidor / USD)	1.332

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo de gestión del proyecto

Según los reportes de la Subsecretaría de Innovación de las Finanzas Públicas, para fines de cálculo de los costos evitados del proyecto se ha identificado a 6.420 usuarios demandantes, cuya remuneración total a nivel nacional asciende a USD 8.553.479 y, finalmente de determina una remuneración promedio de USD 1.332, valores que servirán para monetizar los costos evitados relacionados con el porcentaje de incidencia por el no uso de los sistemas tecnológicos.

- **No uso de sistemas tecnológicos** por falla de infraestructura tecnológica.

Tabla 63 Porcentaje de actividades laborables no dependientes de los sistemas informáticos

Servidor	Día 1	Día 2	Día 3	Día 4	Día 5	Día 6	Día 7	Día 8	Día 9	Día 10
172.27.3.210	60%	61%	93%	71%	93%	50%	48%	57%	70%	76%
172.27.3.211	65%	75%	60%	85%	60%	84%	60%	70%	65%	74%
172.27.3.212	50%	60%	80%	60%	85%	60%	78%	55%	60%	70%
172.27.3.213	75%	62%	85%	65%	65%	50%	50%	56%	50%	81%
172.27.3.214	62%	73%	50%	70%	68%	75%	63%	57%	95%	87%
172.27.3.215	82%	71%	65%	60%	75%	60%	59%	67%	60%	60%
Promedio										**67%**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo de gestión del proyecto

Mediante información histórica se ha identificado que el 67% en promedio de las actividades diarias de los usuarios desarrollan sin mayor dependencia de los sistemas informáticos del Ministerio de Economía y Finanzas.

Tabla 64 Porcentaje de actividades laborables dependientes de los sistemas informáticos

Servidor	Día 1	Día 2	Día 3	Día 4	Día 5	Día 6	Día 7	Día 8	Día 9	Día 10
172.27.3.210	40%	39%	7%	29%	7%	50%	52%	43%	30%	24%
172.27.3.211	35%	25%	40%	15%	40%	16%	40%	30%	35%	26%
172.27.3.212	50%	40%	20%	40%	15%	40%	22%	45%	40%	30%
172.27.3.213	25%	38%	15%	35%	35%	50%	50%	44%	50%	19%
172.27.3.214	38%	27%	50%	30%	32%	25%	37%	43%	5%	13%
172.27.3.215	18%	29%	35%	40%	25%	40%	41%	33%	40%	40%
Promedio										**33%**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo de gestión del proyecto

Mientras que, según los datos se deducen que el 33% en promedio de las actividades laborales con **dependencia muy directa** de los sistemas informáticos, por lo que se reflejara en demoras, retraso y tiempo improductivo.

En resumen, si consideramos, que los usuarios de los sistemas tecnológicos realizan sus actividades regulares al 100% y en el caso de existir falla de la infraestructura tecnológica, sus actividades laborales podrían reducirse al 67%. Es decir, que podría existir un 33% de pérdida de tiempo en horario laboral relacionada al riesgo por la desactualización de la infraestructura tecnológica, lo cual impacta directamente en la prestación de servicios institucionales del MEF a las entidades del sector público.

5.3.2 Identificación y valoración de la inversión total, costos de operación y mantenimiento, ingresos y beneficios

El cálculo de la inversión total, costos de operación y mantenimiento ingresos se expresa en el numeral 5.2.2.

Para el cálculo de los **ahorros generados** para el periodo de 2023-2027 se considera el Porcentaje de no uso de sistemas tecnológicos por falla de infraestructura tecnológica multiplicado por el costo de los usuarios de los sistemas tecnológicos (Sueldo promedio * Número de usuarios) conforme se detalla a continuación:

Tabla 65 Cálculo de ahorro generado por actualización de la infraestructura tecnológica

Denominación	Vigencia del Proyecto				
	2023	2024	2025	2026	2027
Brecha promedio de reducción del riesgo	-60%	-46%	-32%	-14%	0%
Porcentaje deducible de no contar con infraestructura (1 + brecha promedio)	40%	54%	68%	86%	100%
Remuneración promedio de usuarios de sistemas tecnológicos (USD 1332,32) en USD. en relación con el porcentaje deducible	538,26	722,12	905,98	1.151,12	1.332,32
Remuneración total usuarios de sistemas tecnológicos (6420) en USD. en relación con remuneración promedio	3.455.605,59	4.635.985,72	5.816.365,85	7.390.206,02	8.553.479,19
Costo evitado por no uso de sistemas tecnológicos (33%) en relación con la remuneración total de usuarios	**1.140.349,85**	**1.529.875,29**	**1.919.400,73**	**2.438.767,99**	**2.822.648,13**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo de gestión del proyecto

Se ha calculado que el costo evitado del proyecto *"Actualización tecnológica para el fortalecimiento de las finanzas públicas"* para el período 2023-2027 asciende a USD 9.851.041,98.

5.3.3 Flujo económico

Con análisis de beneficios identificado y cuantificado en numeral 5.3.2 se han estimado los valores de beneficios e inversiones se presenta el cálculo del flujo económico.

Tabla 66 Flujo económico

Denominación	Año 0	Año 1	Año 2	Año 3	Año 4
	2023	2024	2025	2026	2027
BENEFICIOS (US Corrientes) (a)	**1.140.349,85**	**1.529.875,29**	**1.919.400,73**	**2.438.767,99**	**2.822.648,13**
Costo evitado por no uso de sistemas tecnológicos en USD	1.140.349,85	1.529.875,29	1.919.400,73	2.438.767,99	2.822.648,13
EGRESOS (b)	**5.162.171,02**	**1.521.968,82**	**-**	**-**	**-**
INVERSIÓN	**5.162.171,02**	**1.521.968,82**	**-**	**-**	**-**
A.1.1 Fortalecimiento de los equipos balanceadores de enlaces, DNS y aplicaciones para el Centro de Datos Principal del Ministerio de Economía y Finanzas	689.562,24	295.526,68	-	-	-
A.1.2 Fortalecimiento de los equipos de seguridad firewall perimetral y firewall IPS de Data Center para el Centro de Datos Principal	641.442,90	274.904,10	-	-	-
A.1.3 Adquisición de Infraestructura para el reforzamiento de conectividad LAN del Centro de Datos Principal del Ministerio de Economía y Finanzas	431.305,65	184.845,28	-	-	-
A.1.4 Adquisición de Infraestructura y Servicio para el reforzamiento de la nube privada	1.558.312,88	-	-	-	-
A.1.5 Adquisición de una solución integral de gestión de respaldos para el Ministerio de Economía y Finanzas	1.282.457,59	549.624,68	-	-	-
A.2.1 Consultoría e implementación de la actualización de la versión de la Nube Privada	6.000,00	54.000,00	-	-	-
IVA	553.089,75	163.068,09			
FLUJO DE CAJA (a-b)	**-4.021.821,17**	**7.906,46**	**1.919.400,73**	**2.438.767,99**	**2.822.648,13**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo gestión del proyecto

El flujo de caja expresa la diferencia de beneficios e inversiones del proyecto, para el 2023 es flujo es negativo, entras que para el 2024, 2025, 2026 y 2027 son positivos.

5.3.4 Indicadores económicos

Para la evaluación económica se ha considerado los siguientes indicadores económicos:

Tabla 67 Indicadores económicos

Parámetros de evaluación financiera	Valores
Tasa de descuento (TD)	12%
Valor Actual Neto (VAN)	1.045.083,48
Tasa interna de retomo (TIR)	21%
Relación beneficio costo (B/C)	1.16

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo gestión del proyecto

Para la evaluación financiera se ha considerado un horizonte del proyecto por un periodo de 5 años (2023 – 2027) y una tasa de descuento del 12%, con estas consideraciones se ha obteniendo el valor actual neto por un valor de 1.045.083,48, una tasa interna de retorno del 21% aceptable y relación beneficio-costo de 1.16 son aspectos positivos y, por consiguiente, los indicadores son viables para la puesta en marcha del proyecto para la *"Actualización tecnológica para el fortalecimiento de las finanzas públicas"*.

5.4 Viabilidad Ambiental y Sostenibilidad Social

5.4.1 Análisis de impacto ambiental y riesgos

5.4.1.1 Impacto Ambiental

Por su naturaleza, el proyecto no tiene afectación directa al ambiente y por lo tanto no requiere de un estudio de impacto ambiental; sin embargo, uno de los objetivos busca la racionalización del uso del papel, al ser un proyecto eminentemente tecnológico en el que todos sus entornos son digitales, incluso los respaldos de información.

5.4.1.2 Riesgos

Uno de los riesgos levantados para este proyecto es la demora o la no obtención de todas las autorizaciones de todos las entidades o Entes Rectores para la ejecución del proyecto, lo que impactaría directamente en la factibilidad de realizarlo.

Los riesgos tecnológicos y de servicio se describen a continuación:

- El daño físico en los equipos de seguridad causaría un corte en el flujo de las comunicaciones y la red estaría expuesta ante cualquier ataque de ciberseguridad.
- El daño físico del equipo de comunicaciones causaría la incapacidad total de acceder a las aplicaciones del SINFIP.
- El daño físico del equipo balanceador externo causaría que los usuarios desde el internet no puedan acceder a las aplicaciones y servicios del SINFIP.
- El daño físico del equipo de balanceo interno provocaría indisponibilidad de acceso de todos los usuarios a las aplicaciones y servicios del SINFIP; así como se perdería la comunicación entre los servidores que dan servicio a las aplicaciones.
- La capacidad limitada para la asignación de recursos de procesador, memoria y disco que tiene la actual infraestructura de Nube Privada afectaría el rendimiento, y nuevos requerimientos de las aplicaciones y servicios del SINFIP.
- El daño físico en la actual infraestructura de Nube Privada provocaría la suspensión total de las aplicaciones y servicios del Sistema Nacional de las Finanzas Públicas del Ecuador.
- El daño físico de la plataforma de respaldos provocaría que no se pueda generar o restaurar los respaldos, de la toda la información crítica del Sistema de las Finanzas Públicas
- La no generación de un respaldo causaría en el caso de un incidente o contingencia la imposibilidad de subir el servicio de las aplicaciones o el de recuperar información crítica afectada.

5.4.2 Sostenibilidad Social

Por su naturaleza, el proyecto no cuenta con actividades de mantenimiento o incremento de capital social; sin embargo, apoya a que todas las transacciones financieras que las entidades a través de los usuarios realizan para la gestión de su entidad en los sistemas, se mantengan operativas, aportando a los ciudadanos y a los servicios públicos.

6. FINANCIAMIENTO Y PRESUPUESTO

Para la ejecución de este proyecto, se cuenta con el financiamiento del Banco Interamericano de Desarrollo –BID-, a través del Préstamo No. 4812/OC-EC otorgado para ejecución del "*Programa de Modernización de la Administración Financiera*" con CUP 81300000.0000.384365. El proyecto forma parte del primer componente del crédito.

El monto asignado asciende a USD 6.684.139,84 al proyecto. El detalle del uso se describe en la siguiente tabla:

Tabla 68 Fuentes de Financiamiento (dólares)

Componentes /Rubros	Grupo de gasto	FUENTES DE FINANCIAMIENTO (dólares)						TOTAL
		Externas		Internas				
		Crédito	Cooperación	Crédito	Fiscales	Autogestión	A. Comunidad	
Componente 1: Fortalecimiento de la infraestructura tecnológica del SINFIP (Hardware)								
Act. 1.1 Fortalecimiento de los equipos balanceadores de enlaces, DNS y aplicaciones para el Centro de Datos Principal del Ministerio de Economía y Finanzas	84	1.103.299,59	-	-	-	-	-	1.103.299,59
Act. 1.2 Fortalecimiento de los equipos de seguridad firewall perimetral y firewall IPS de Data Center para el Centro de Datos Principal	84	1.026.308,64	-	-	-	-	-	1.026.308,64
Act. 1.3 Adquisición de Infraestructura para el reforzamiento de conectividad LAN del Centro de Datos Principal del Ministerio de Economía y Finanzas	84	690.089,04	-	-	-	-	-	690.089,04
Act. 1.4 Adquisición de Infraestructura y Servicio para el reforzamiento de la nube privada	84	1.745.310,43	-	-	-	-	-	1.745.310,43
Act. 1.5 Adquisición de una solución integral de gestión de respaldos para el Ministerio de Economía y Finanzas	84	2.051.932,14	-	-	-	-	-	2.051.932,14
Componente 2: Reducción de la brecha tecnológica y operativa del MEF (Software)								
Act. 2.1 Consultoría e implementación de la actualización de la versión de la Nube Privada	73	**67.200,00**	-	-	-	-	-	67.200,00
Total		**6.684.139,84**	-	-	-	-	-	**6.684.139,84**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo gestión del proyecto

7. ESTRATEGIA DE EJECUCIÓN

7.1 Estructura Operativa

El Ministerio de Economía y Finanzas ejecutará el proyecto a través de la Dirección Nacional de Operaciones de las Finanzas Públicas, que pertenece a la Subsecretaría de Innovación de las Finanzas Públicas; a continuación, se explica su estructura orgánica, y para mayor referencia se adjunta el Estatuto Orgánico Funcional del Ministerio (Anexo x):

Subsecretaría de Innovación de las Finanzas Públicas, está formada por 4 direcciones:

- Dirección Nacional de Innovación Conceptual y Normativa
- Dirección Nacional de Sistemas de Información de las Finanzas Públicas
- **Dirección Nacional de Operaciones de los Sistemas de las Finanzas Públicas**
- Dirección Nacional del Centro de Servicios

Según el Acuerdo Ministerial N° 254, establece entre otros, la misión y responsabilidades de las áreas del Ministerio; a continuación, se detalla las áreas ejecutoras del proyecto:

Subsecretaría de Innovación de las Finanzas Públicas

a) Misión

Innovar de manera permanente los conceptos, metodologías, procesos, tecnologías y servicios inherentes al Sistema Nacional de las Finanzas Públicas, para contribuir a una mayor eficiencia y efectividad en la gestión de las finanzas públicas.

b) Atribuciones y responsabilidades

1. Impulsar e implantar las iniciativas de innovación y modernización del Sistema Nacional de las Finanzas Públicas;
2. Promover que la innovación conceptual de las finanzas públicas vaya alineada a las nuevas tecnologías de información;
3. Planificar, definir estrategias, administrar y optimizar el Sistema de Administración Financiera y todas sus aplicaciones;
4. Planificar, promover, supervisar y ejecutar la entrega eficiente de los servicios que el Sistema Nacional de las Finanzas Públicas que ofrece a los usuarios internos y externos;
5. Establecer relaciones estratégicas con otras entidades públicas para integrar procesos comunes;
6. Proveer a los funcionarios públicos capacitación y asistencia técnica, conceptual y operativa en finanzas públicas y en el uso del Sistema de Administración Financiera y todas sus aplicaciones;
7. Gestionar el portafolio de proyectos de la subsecretaría y su ejecución;
8. Realizar análisis y planificación de gestión de riesgos y seguridad de la información;
9. Administrar el sistema oficial de la información de las finanzas públicas y su amplia difusión.
10. Las demás previstas en las leyes y reglamentos que rigen la materia; y, las que le delegue la autoridad.

Dirección Nacional de Operaciones de los Sistemas de las Finanzas Públicas

a) Misión

Garantizar la operación, seguridad y disponibilidad de la infraestructura tecnológica que soporta a las aplicaciones de software del Sistema Nacional de Finanzas Públicas en cumplimiento a los acuerdos de niveles de servicio establecidos.

b) Atribuciones y responsabilidades

1. Garantizar que la infraestructura de tecnología de información satisfaga las necesidades de negocio del SINFIP y los requerimientos técnicos de las aplicaciones;
2. Promover y garantizar el uso del marco de referencia para el diseño y operación de los servicios para reducir el riesgo, mejorar la calidad y asegurar la exactitud de las cargas de trabajo estimadas
3. Gestionar la disponibilidad, capacidad, continuidad de operaciones, seguridad e instalaciones de tecnología de información y de los sistemas del SINFIP;
4. Participar en la definición de SLAs;
5. Administrar la plataforma de hardware y software base;
6. Administrar la base de datos de gestión de la configuración (CMDB);
7. Gestionar los problemas, cambios, configuración y versionado de plataforma;
8. Monitorear las operaciones y la producción de los sistemas;
9. Gestión de riesgos y de seguridad de infraestructura tecnología de información y de los sistemas del SINFIP;
10. Coordinar la entrega de servicios con las otras direcciones;
11. Las demás previstas en las leyes y reglamentos que rigen la materia; y, las que le delegue la autoridad.

c) Productos

1. Portafolio de Servicios de tecnología de la información.
2. Plan, políticas y reportes de seguridad de infraestructura.
3. Plan, líneas de base, umbrales, alarmas y base de datos de la capacidad de Infraestructura.
4. Planes de continuidad y recuperaciones de operaciones/tecnología de información.
5. Plan de reducción del riesgo.
6. Plan, diseño y calendarios de la disponibilidad/recuperación.
7. Plan de mantenimiento de las instalaciones.
8. Base de datos de gestión de la configuración actualizada.
9. Informe de administración técnica de los contratos.

7.2 Arreglos institucionales y modalidad de ejecución

Se detalla en el siguiente cuadro la modalidad de ejecución para este proyecto, que es directa, ya que, este Ministerio, a través de la Subsecretaría de Innovación de las Finanzas Públicas, lo va a ejecutar:

Tabla 69 Arreglos Institucionales

Tipo de Ejecución		Instituciones Involucradas
Directa (D) o Indirecta (I)	**Tipo de arreglo**	
Ejecución directa del Ministerio de Economía y Finanzas (D)		

7.3 Cronograma valorado por componentes y actividades

A continuación, se detalla el cronograma valorado plurianual por componente y nivel de detalle por actividad, con la finalidad de valorar las acciones a ser desarrolladas en el proyecto cronológicamente:

Tabla 70 Cronograma valorado por componente y fuente de financiamiento (dólares)

Componentes /Rubros	CRONOGRAMA VALORADO POR COMPONENTE Y FUENTE DE FINANCIAMIENTO (dólares)												TOTAL
	Externas		Internas										
	Crédito		Cooperación		Crédito		Fiscales		Autogestión		A.Com.		
	2023	2024	2023	2024	2023	2024	2023	2024	2023	2024	2023	2024	
Componente 1: Fortalecimiento de la infraestructura tecnológica del SINFIP (Hardware)	**5.155.451,02**	**1.461.488,82**	-	-	-	-	-	-	-	-	-	-	**6.616.939,84**
Act. 1.1 Fortalecimiento de los equipos balanceadores de enlaces, DNS y aplicaciones para el Centro de Datos Principal del Ministerio de Economía y Finanzas	772.309,71	330.989,88	-	-	-	-	-	-	-	-	-	-	1.103.299,59
Act. 1.2 Fortalecimiento de los equipos de seguridad firewall perimetral y firewall IPS de Data Center para el Centro de Datos Principal	718.416,05	307.892,59	-	-	-	-	-	-	-	-	-	-	1.026.308,64
Act. 1.3 Adquisición de Infraestructura para el reforzamiento de conectividad LAN del Centro de Datos Principal del Ministerio de Economía y Finanzas	483.062,33	207.026,71	-	-	-	-	-	-	-	-	-	-	690.089,04
Act. 1.4 Adquisición de Infraestructura y Servicio para el reforzamiento de la nube privada	1.745.310,43	-	-	-	-	-	-	-	-	-	-	-	1.745.310,43
Act. 1.5 Adquisición de una solución integral de gestión de respaldos para el Ministerio de Economía y Finanzas	1.436.352,50	615.579,64	-	-	-	-	-	-	-	-	-	-	2.051.932,14
Componente 2: Reducción de la brecha tecnológica y operativa del MEF (Software)	**6.720,00**	**60.480,00**	-	-	-	-	-	-	-	-	-	-	**67.200,00**
Act. 2.1 Consultoría e implementación de la actualización de la versión de la Nube Privada	6.720,00	60.480,00	-	-	-	-	-	-	-	-	-	-	67.200,00
Total	**5.162.171,02**	**1.521.968,82**	-	-	-	-	-	-	-	-	-	-	**6.684.139,84**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo gestión del proyecto

A continuación, se detalla el cronograma valorado para el año 2023 primer año, mensualizado, a nivel de grupo de gasto, por componente y nivel de detalle por actividad, con la finalidad de valorar las acciones a ser desarrolladas en el proyecto cronológicamente:

Tabla 71 Cronograma valorado por componente y fuente de financiamiento (dólares) Año 2022

			2023																
		Grupo Gasto	Ene	Feb	Mar	Ab	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Sub Total				Total Proyecto
															Contrato/Planificado	IVA	Total Fiscal	Total Externo	
C1	**Fortalecimiento de la infraestructura tecnológica del SINFIP (Hardware)**		-	-	2.646.775,94	-	-	-	-	-	-	1.985.081,95	-	523.593,13	4.603.081,26	552.369,75	-	5.155.451,02	5.155.451,02
act. 1.1	Fortalecimiento de los equipos balanceadores de enlaces, DNS y aplicaciones para el Centro de Datos Principal del Ministerio de Economía y Finanzas	84	-	-	441.319,84	-	-	-	-	-	-	330.989,88	-	-	689.562,24	82.747,47	-	772.309,71	772.309,71
act. 1.2	Fortalecimiento de los equipos de seguridad firewall perimetral y firewall IPS de Data Center para el Centro de Datos Principal	84	-	-	410.523,46	-	-	-	-	-	-	307.892,59	-	-	641.442,90	76.973,15	-	718.416,05	718.416,05
act. 1.3	Adquisición de Infraestructura para el reforzamiento de conectividad LAN del Centro de Datos Principal del Ministerio de Economía y Finanzas	84	-		276.035,62	-	-	-	-	-	-	207.026,71	-	-	431.305,65	51.756,68	-	483.062,33	483.062,33
act. 1.4	Adquisición de Infraestructura y Servicio para el reforzamiento de la nube privada	84	-		698.124,17	-	-	-	-	-	-	523.593,13	-	523.593,13	1.558.312,88	186.997,55	-	1.745.310,43	1.745.310,43
act. 1.5	Adquisición de una solución integral de gestión de respaldos para el Ministerio de Economía y Finanzas	84	-		820.772,86	-	-	-	-	-	-	615.579,64	-	-	1.282.457,59	153.894,91	-	1.436.352,50	1.436.352,50
C2	**Reducción de la brecha tecnológica y operativa del MEF (Software)**		-	-	-	-	-	-	-	-	-	6.720,00	-	-	6.000,00	720,00	-	6.720,00	6.720,00
act. 2.1	Consultoría e implementación de la actualización de la versión de la Nube Privada	73	-	-	-	-	-	-	-	-	-	6.720,00	-	-	6.000,00	720,00	-	6.720,00	6.720,00
	Sub Total		-	-	2.646.775,94	-	-	-	-	-	-	1.991.801,95	-	523.593,13	4.609.081,26	553.089,75	-	5.162.171,02	**5.162.171,02**
	Total		-	-	2.646.775,94	-	-	-	-	-	-	1.991.801,95	-	523.593,13				**5.162.171,02**	

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP

Elaborado por: Equipo gestión del proyecto

7.4 Demanda pública nacional plurianual

7.4.1 Determinación de la demanda pública nacional plurianual

A continuación, se detalla en la siguiente tabla la demanda pública nacional e internacional plurianual para el proyecto:

Tabla 72 Demanda Pública Plurianual

Código Categoría CPC	Tipo Compra (Bien, obra, servicio)	Detalle del producto (especificación técnica)	Cantidad anual	Unidad (metro, litro, etc.)	Costo Unitario (Dólares)	Origen de los Insumos (USD Y %)		Monto a contratar		TOTAL
						Nacional	Importado	2023	2024	
47211021	Bien	Fortalecimiento de los equipos balanceadores de enlaces, DNS y aplicaciones para el Centro de Datos Principal del Ministerio de Economía y Finanzas	1	Unidad	1.103.299,59	0%	100%	772.309,71	330.989,88	**1.103.299,59**
47211021	Bien	Fortalecimiento de los equipos de seguridad firewall perimetral y firewall IPS de Data Center para el Centro de Datos Principal	1	Unidad	1.026.308,64	0%	100%	718.416,05	307.892,59	**1.026.308,64**
47211021	Bien	Adquisición de Infraestructura para el reforzamiento de conectividad LAN del Centro de Datos Principal del Ministerio de Economía y Finanzas	1	Unidad	690.089,04	0%	100%	483.062,33	207.026,71	**690.089,04**
452300049	Bien	Adquisición de Infraestructura y Servicio para el reforzamiento de la nube privada	1	Unidad	1.745.310,43	0%	100%	1.745.310,43	-	**1.745.310,43**

Código Categoría CPC	Tipo Compra (Bien, obra, servicio)	Detalle del producto (especificación técnica)	Cantidad anual	Unidad (metro, litro, etc.)	Costo Unitario (Dólares)	Origen de los Insumos (USD Y %)		Monto a contratar		TOTAL
						Nacional	Importado	2023	2024	
45230004	Bien	Adquisición de una solución integral de gestión de respaldos para el Ministerio de Economía y Finanzas	1	Unidad	2.051.932,14	0%	100%	1.436.352,50	615.579,64	**2.051.932,14**
83141	Servicio	Consultoría e implementación de la actualización de la versión de la Nube Privada	1	Unidad	67.200,00	0%	100%	6.720,00	60.480,00	**67.200,00**
TOTAL					**6.684.139,84**			**5.162.171,02**	**1.521.968,82**	**6.684.139,84**

Fuente: Subsecretaría de Innovación de las Finanzas Públicas-DNOSFP
Elaborado por: Equipo gestión del proyecto

8. ESTRATEGIA DE SEGUIMIENTO Y EVALUACIÓN

8.1 Seguimiento a la ejecución

El Ministerio de Economía y Finanzas realizará el seguimiento a través de la Subsecretaría de Innovación de las Finanzas Públicas, específicamente de la Dirección Nacional de Operaciones de los Sistemas de las Finanzas Públicas, con un equipo especializado a través de administradores de contrato para las actividades definidas en el proyecto, con las responsabilidades señaladas en la Ley Orgánica del Sistema Nacional de Contratación Pública, Artículo 80 *"Responsable de la administración del contrato.- El supervisor y el fiscalizador del contrato son los responsables de tomar todas las medidas necesarias para su adecuada ejecución, con estricto cumplimiento de sus cláusulas, programas, cronogramas, plazos y costos previstos…"*

8.2 Evaluación de resultados e impactos

En el proyecto se realizará la evaluación de resultados, para analizar si se alcanzaron las metas propuestas con base en los indicadores establecidos en la Matriz de Marco Lógico, tomando en cuenta el porcentaje de disponibilidad de infraestructura tecnológica para los usuarios de los sistemas de las Finanzas el cual se obtendrá de la herramienta de monitoreo de la infraestructura tecnológica.

En cuanto a la evaluación de impactos se realizará conforme los lineamientos definidos por la Secretaría Técnica de Planificación "Planifica Ecuador".

8.3 Actualización de la línea base

Por la naturaleza de este proyecto se actualizará la línea base al implementar la infraestructura en el primer año, ya que abarca más del 70% de implementación del proyecto, y se podrán visualizar cambios.

9. ANEXOS

9.1 Autorizaciones ambientales otorgadas por el Ministerio de Ambiente y otros según corresponda

Este punto no aplica por tratarse de un proyecto de desarrollo de software que no tiene ninguna afectación directa al medio ambiente.

9.2 Certificaciones técnicas, costos, disponibilidad de financiamiento y otras

Anexo 1: Estructura Orgánica del Ministerio de Finanzas AM 254
Anexo 2: Informes
Anexo 3: Contrato de Préstamo N° 4812/OC-EC
Anexo 4: Autorización MINITEL