CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA - COPNIA

FICHA DE PROGRAMACIÓN PROYECTO DE INVERSIÓN 2025

APROPIACIÓN (GASTOS)

INFORMACIÓN DEL PROYECTO

CIUDAD:	BOGOTA	FECHA:	23/09/2024

NOMBRE DEL PROYECTO:	Proyecto de inversión para la renovación de Firewalls, switches y routers en las regionales, seccionales y sede nacional de la entidad.
NOMBRE DE QUIEN PROYECTA LA FICHA DE INVERSIÓN:	MARICELA OYOLA MARTINEZ
CARGO DE QUIEN PROYECTA FICHA DE INVERSIÓN:	Subdirectora Administrativa y Financiera

FECHA ESTIMADA DE INICIO DEL PROYECTO:	mar-24	FECHA ESTIMADA DE TERMINACIÓN DEL PROYECTO:	ago-24

IDENTIFICACIÓN:

La renovación de los switches y routers a nivel nacional en COPNIA es imprescindible debido a la obsolescencia tecnológica y el fin de vida útil de los equipos actuales según lo determinado por el fabricante CISCO y FORTINET. Esta situación compromete la estabilidad, seguridad y eficiencia de la red de la entidad, afectando directamente la operatividad de los servicios críticos. La falta de actualizaciones de seguridad y soporte técnico pone en riesgo la integridad de los datos y la continuidad del negocio, por lo que es necesario actualizar a equipos modernos que cumplan con los estándares actuales y soporten el crecimiento futuro de la entidad.

ANTECEDENTES:

Hechos que llevaron a la formulación de la necesidad:

1. Obsolescencia tecnológica: Los equipos de red actuales, como switches y routers, han superado su ciclo de vida útil según las especificaciones del fabricante, CISCO y FORTINET. Esto los convierte en obsoletos y más vulnerables a fallos y problemas de rendimiento.

2. Fin de vida útil de los equipos: El fabricante ha declarado oficialmente que los equipos ya no recibirán soporte técnico ni actualizaciones de seguridad, lo que aumenta los riesgos para la red de COPNIA y compromete su funcionalidad.

3. Compromiso de estabilidad y seguridad: La falta de actualizaciones de seguridad y parches de vulnerabilidad en los equipos actuales compromete la integridad de la red, aumentando la probabilidad de ataques cibernéticos o fallos de seguridad que puedan exponer datos sensibles.

4. Afectación a la operatividad de los servicios críticos: La red es fundamental para la operatividad de COPNIA y, debido a la inestabilidad de los equipos antiguos, los servicios críticos de la entidad se ven afectados, lo que repercute directamente en la productividad y en la capacidad de prestar servicios de calidad.

5. Riesgo para la continuidad del negocio: La falta de soporte técnico y las crecientes fallas de los equipos pueden derivar en interrupciones importantes, afectando la continuidad operativa de COPNIA y exponiendo la entidad a pérdidas económicas y reputacionales.

6. Necesidad de modernización: Para garantizar la estabilidad, seguridad y capacidad de crecimiento de la red de COPNIA, es imprescindible la adquisición de equipos modernos que cumplan con los estándares tecnológicos actuales y permitan un escalamiento acorde a las necesidades futuras de la entidad.

7. Soporte al crecimiento futuro: COPNIA prevé un crecimiento en sus operaciones y en la cantidad de datos y usuarios que soporta su red, lo cual requiere una infraestructura de red que pueda acompañar y facilitar dicho crecimiento, algo que los equipos actuales no pueden ofrecer.

APROPIACIÓN (GASTOS)

DESTINATARIO:

1. Funcionarios de COPNIA: Todo el personal administrativo y operativo de la entidad se beneficiará de una red más estable y segura, mejorando su productividad y facilitando su trabajo diario.

2. Ingenieros y profesionales registrados: Los usuarios que interactúan con los servicios en línea de COPNIA podrán acceder de manera más eficiente a los sistemas, con menor riesgo de interrupciones, lo que facilita la realización de trámites y consultas.

3. Entidades asociadas y contratistas: Las entidades y organizaciones que colaboran o interactúan con COPNIA verán mejorada la conectividad y la seguridad en sus comunicaciones y transacciones.

4. Proveedores de tecnología y servicios: Las empresas encargadas de proveer soluciones tecnológicas se beneficiarán de una mejor infraestructura de red que soporte los servicios y soluciones que brindan a la entidad.

5. Usuarios de los sistemas de información de COPNIA: Cualquier usuario que acceda a las plataformas digitales, incluidas consultas públicas y privadas, será beneficiado con tiempos de respuesta más rápidos y mayor seguridad.

6. Administradores de la plataforma tecnológica de COPNIA: Tendrán una mejor capacidad de monitoreo y control de la red, lo que les permitirá tomar decisiones informadas y garantizar la continuidad operativa.

7. Ciudadanía en general: La mejora en la infraestructura de red de COPNIA permitirá un servicio más eficiente y seguro, lo que indirectamente beneficiará a todos aquellos que dependen de la calidad de los servicios ofrecidos por la entidad.

MARCO LEGAL, CONCEPTUAL Y TÉCNICO

1. Marco Legal Colombiano
El marco legal aplicable para la renovación de la infraestructura tecnológica en entidades públicas como COPNIA se rige por las siguientes leyes y normativas:
•Decreto 1078 de 2015 (Decreto Único Reglamentario del Sector TIC): Regula la infraestructura tecnológica, las telecomunicaciones y las políticas para la implementación de tecnologías de la información en entidades del Estado, con énfasis en garantizar la seguridad y eficiencia de los sistemas.
•Ley 1581 de 2012 (Ley de Protección de Datos Personales): Establece las reglas para el tratamiento de datos personales, lo cual es relevante al implementar nuevas infraestructuras tecnológicas que manejen datos sensibles.
•Ley 1341 de 2009 (Ley TIC): Promueve el acceso a las tecnologías de la información y las comunicaciones y el uso eficiente de los recursos del espectro electromagnético. Esta ley también establece los estándares para la modernización de las telecomunicaciones en el país.

2. Parte Técnica del Reemplazo de Firewalls y Equipos de Red
Reemplazo de Firewalls Fortinet 240D por obsolescencia
Justificación técnica: Los 2 firewalls Fortinet 240D han alcanzado su vida útil y no cuentan con soporte técnico ni actualizaciones de firmware del fabricante, lo que los hace vulnerables a ciberataques y fallos de seguridad. Se propone el reemplazo por modelos con capacidades superiores que ofrece mejor rendimiento, protección de amenazas avanzadas y soporte continuo de actualizaciones.
Switches: Los 21 switches actuales deben ser reemplazados por modelos modernos que soporten características avanzadas como:
Administración en la nube
Gigabit Ethernet: Mayor velocidad y capacidad para manejar tráfico intenso de datos.
PoE+ (Power over Ethernet Plus): Alimentación de dispositivos como teléfonos IP y puntos de acceso inalámbrico a través del cableado Ethernet.
Stacking: Capacidad de conectar múltiples switches para simplificar la administración y aumentar la redundancia.
Capacidades avanzadas de enrutamiento, seguridad y escalabilidad.
Routers: Los 16 routers obsoletos de las sedes remotas deben ser reemplazados por equipos Firewall más robustos que soporten mayores velocidades, mejor conectividad WAN y manejo avanzado de tráfico.
Modelo que ofrezca alta capacidad de procesamiento, administración en nube, conectividad WAN, funcionalidades de seguridad integradas y soporte para redes virtuales.

3. Fases del proyecto
Fase 1: Planeación
Fase 2: Adquisición
Fase 3: Implementación
Fase 4: Pruebas y Capacitación
Fase 5: Cierre

APROPIACIÓN (GASTOS)

OBJETIVO GENERAL DEL PROYECTO:

Actualizar y modernizar la infraestructura de red de COPNIA mediante el reemplazo de los equipos obsoletos, incluyendo switches, routers y firewalls, en las 17 seccionales, regionales y la sede nacional, con el fin de garantizar la estabilidad, seguridad y eficiencia en la operatividad de los servicios críticos, así como asegurar la continuidad del negocio y el cumplimiento de los estándares tecnológicos actuales, habilitando la red para soportar el crecimiento futuro de la entidad.

OBJETIVOS ESPECÍFICOS DEL PROYECTO:

• Reemplazar los firewalls Fortinet 240D por equipos modernos que ofrezcan administración en nube, mayor capacidad de procesamiento, seguridad avanzada y soporte continuo, garantizando la protecció frente a amenazas cibernéticas y la estabilidad de la red.

• Reemplazar los switches en las 17 seccionales/Regionales y la sede nacional por dispositivos más eficientes, que permitan administración en nube, con mayor capacidad de transmisión de datos funcionalidades avanzadas como PoE+ y stacking, que permitan optimizar la conectividad y el rendimiento de la red.

• Reemplazar los 16 Router en las seccionales/Regionales por equipos Firewall modernos que ofrezcan administración en nube, mayor capacidad de procesamiento, seguridad avanzada y soporte continuo garantizando la protección frente a amenazas cibernéticas y la estabilidad de la red.

• Asegurar la continuidad operativa de COPNIA mediante la implementación de equipos de red con alta disponibilidad, redundancia y capacidad de escalamiento, evitando fallos o interrupciones en los servicio críticos de la entidad.

•Garantizar el cumplimiento de los estándares de seguridad y normativas vigentes mediante la actualización de la infraestructura tecnológica, protegiendo la integridad de los datos y sistemas de COPNIA.

• Optimizar el rendimiento de la red para soportar el crecimiento futuro de la entidad, mejorando la capacidad de procesamiento y transmisión de datos, y permitiendo la expansión de usuarios y servicios si comprometer la calidad de la conectividad.

• Monitorear y ajustar el rendimiento de la red post-implementación, realizando pruebas y optimizaciones para garantizar que los equipos instalados cumplan con los objetivos de seguridad, estabilidad

OBJETIVO ESTRATÉGICO (DEL PLAN ESTRATÉGICO INSTITUCIONAL)

Consolidar el Modelo de Gestión de la entidad para mejorar la prestación de los servicios misionales.

OBJETIVO ESPECIFICO (DEL PLAN ESTRATÉGICO)+B17:P26

Mejorar la infraestructura física y el hardware del COPNIA para garantizar una adecuada prestación del servicio.

RECURSOS INTERNOS REQUERIDOS

ÍTEM	DESCRIPCIÓN
RECURSO HUMANO	Gerente de proyecto (Suministrado por el proveedor) Ingeniero especialista en implementación de soluciones de red y seguridad (Suministrado por el proveedor) Arquitecto de soluciones de Infraestructura TI (Suministrado por el proveedor) Ingeniero de Soporte y Mantenimiento (Suministrado por el proveedor) Equipo de Soporte Regional (Técnicos de Redes Locales) (Suministrado por el proveedor) Equipo de TIC (Copnia) Oficial de seguridad y privacidad de la información (Copnia) Equipo de contratación (Copnia)
RECURSO FÍSICO	1 Firewall sede nacional 1 Firewall sede Cundinamarca 16 Firewall Sedes Remotas 4 Switch sede nacional 1 Switch sede Cundinamarca 16 switch sedes remotas

APROPIACIÓN (GASTOS)

CRONOGRAMA

ACTIVIDAD	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Fase 1: Planeación Fase 2: Adquisición			X									
Fase 3: Implementación				X	X	X						
Fase 4: Pruebas y Capacitación Fase 5: Cierre							X	X				

PRESUPUESTO DEL PROYECTO VIGENCIA 2021

ORDEN	DESCRIPCIÓN DEL PRODUCTO	CANTIDAD		COSTO	
		NÚMERO	UNIDAD DE MEDIDA	UNITARIO	TOTAL
1	Proyecto de inversión para la renovación de Firewalls, switches y routers en las regionales, seccionales y sede nacional de la entidad	1	1	$ 450.403.111	$ 450.403.111
2					
3					
4					
5					
6					
VALOR GENERAL DEL PROYECTO					**$ 450.403.111**

PRODUCTOS ESPERADOS	FECHA DE ENTREGA
Fase 1: Planeación 1. Documentación del Plan de Proyecto: - Planificación detallada de la renovación de firewalls y switches en todas las sedes. - Cronograma del proyecto. - Asignación de recursos humanos y materiales. - Plan de gestión de riesgos, incluyendo estrategias de mitigación. - Plan de adquisición de equipos (licitaciones, proveedores). 2. Documentación Técnica Inicial: - Especificaciones técnicas de los equipos (firewalls y switches) en todas las sedes. - Inventario de los equipos actuales que serán reemplazados.	MARZO
Fase 2: Adquisición 3. Adquisición de Equipos y licenciamientos para: - 18 firewalls: 1 para la sede nacional, 1 para la sede de Cundinamarca, y 16 para las sedes remotas. - 21 switches: 4 para la sede nacional, 1 para la sede de Cundinamarca, y 16 para las sedes remotas.	MARZO

APROPIACIÓN (GASTOS)

Fase 3: Implementación 5. Instalación de Equipos en la Sede Nacional: - Firewall: Configuración e instalación del nuevo firewall en la sede nacional. - Switches: Instalación y configuración de 4 switches en la sede nacional. - Pruebas iniciales: Pruebas de conectividad, seguridad, y rendimiento en la sede nacional. 6. Instalación de Equipos en la Sede de Cundinamarca: - Firewall: Instalación y configuración del firewall en la sede de Cundinamarca. - Switch: Instalación y configuración del switch en la sede de Cundinamarca. - Pruebas iniciales: Validación de conectividad, seguridad, y rendimiento. 7. Instalación en las Sedes Remotas: - Firewalls: Instalación de los 16 firewalls en las sedes remotas, con configuraciones estandarizadas. - Switches: Instalación de 16 switches en las sedes remotas. - Pruebas de conexión y seguridad en sedes remotas: Validación de la conectividad y funcionamiento de los equipos.	JUNIO
Fase 4: Pruebas y Capacitación 8. Pruebas de Rendimiento y Seguridad: - Pruebas de conectividad: Verificación de que todos los firewalls y switches estén operativos y correctamente integrados en la red. - Simulaciones de ciberataques: Pruebas de los firewalls para validar la protección de la red contra amenazas externas. - Monitoreo del rendimiento de los switches: Asegurar que los switches estén manejando adecuadamente el tráfico de red sin interrupciones. 9. Capacitación del Personal: - Capacitación a los administradores de red de COPNIA sobre el manejo de los nuevos firewalls y switches. - Entrenamiento en la gestión y monitoreo de los equipos mediante herramientas de administración de red. Fase 5: Cierre 10. Informe de Cierre del Proyecto: - Informe detallado de las actividades realizadas, cumplimiento de cronograma y presupuesto. - Resultados de las pruebas de rendimiento y seguridad. - Documentación final de la configuración de todos los equipos instalados. 11. Entrega Oficial de Equipos y Servicios: - Formalización de la entrega de los 18 firewalls y 21 switches instalados y configurados en las sedes correspondientes. - Certificación de que los equipos están operativos y funcionando de acuerdo con los requisitos técnicos. 12. Plan de Soporte y Mantenimiento: - Acuerdo de soporte con el proveedor para garantizar el mantenimiento preventivo y correctivo de los nuevos equipos. - Establecimiento de procedimientos internos para la administración continua de la infraestructura de red.	AGOSTO

RECOMENDACIONES Y OBSERVACIONES:

Para garantizar el éxito del proyecto de renovación de la infraestructura de red en COPNIA, es fundamental realizar una planificación detallada y asegurar una adecuada coordinación entre todas las partes involucradas. Se recomienda establecer un cronograma realista que contemple posibles contingencias, asegurando que haya redundancia en los servicios críticos durante la instalación para evitar interrupciones en las operaciones. Además, es clave realizar pruebas exhaustivas de los equipos antes de su implementación completa, verificando su compatibilidad con la infraestructura actual y su rendimiento bajo condiciones de carga real. La capacitación continua del personal técnico es esencial para asegurar la correcta administración de los nuevos dispositivos. Finalmente, se sugiere mantener un plan de monitoreo y mantenimiento periódico que permita anticiparse a posibles problemas y garantizar la longevidad de la inversión tecnológica.

Nombre y cargo de quién presenta el proyecto: MARICELA OYOLA MARTINEZ
Fecha de programación: 24/09/2024 Subdirectora Administrativa y Financiera