ACTA DE INICIO

Contrato No.	2546 DE 2026		
Objeto del contrato	CONTRATAR LA GESTIÓN INTEGRAL DE LOS SERVICIOS TECNOLÓGICOS DE LA UNP.		
Valor del contrato	VEINTIOCHO MIL CIENTO VEINTIÚN MILLONES QUINIENTOS SETENTA Y OCHO MIL OCHOCIENTOS VEINTIOCHO PESOS M/CTE ($28.121.578.828,00)		
Registro presupuestal	497426	Fecha Registro Presupuestal	5 de junio de 2026
Fecha de firma	viernes, 5 de junio de 2026		
Fecha de inicio ejecución	martes, 30 de junio de 2026		
Fecha de terminación	jueves, 31 de diciembre de 2026		
Póliza Garantía de Cumplimiento- Otros	Número	33-44-101277188	
	Fecha aprobación	17 de junio de 2026	
	Aseguradora	SEGUROS DEL ESTADO	
Póliza Garantía de Responsabilidad civil Extracontractual	Número	33-40-101091297	
	Fecha aprobación	17 de junio de 2026	
	Aseguradora	SEGUROS DEL ESTADO	
Póliza Garantía de Responsabilidad de Riesgos Cibernéticos	Número	900001625548	
	Fecha aprobación	30 de junio de 2026	
	Aseguradora	SEGUROS GENERALES SURAMERICANA S.A	
Contratista	**UNIÓN TEMPORAL SERVICIOS TECNOLÓGICOS SSC**		
	NIT 902.074.972-3		
Supervisor	**JAVIER FRANCISCO RODRÍGUEZ MORENO** CC. 80000431 Jefe de la Oficina de Tecnologías y Sistemas de Información – OTSI (E)		

Entre los suscritos el representante legal de la UT SERVICIOS TECNOLÓGICOS SSC y el supervisor del contrato designado por la Unidad Nacional de Protección - UNP, y una vez verificado el cumplimiento de los requisitos de perfeccionamiento y legalización del contrato, así como, de las condiciones exigidas para iniciar la ejecución del contrato, se deja constancia mediante la presente acta de inicio del plazo de ejecución del contrato y de la activación de las líneas de servicio así:

1.1 Mesa de Ayuda y Soporte en sitio (Servicios Centrales) // 1.2 Soporte Remoto y en Sitio (Línea de Emergencia Vida 103) // 2.1.2 Colocación // 2.1.3 Servicios Administrados SO y BD //

2.1.4 Cross Conexiones // 2.1.5 Renovación soporte hardware de los activos de la colocación // 2.1.6 Administración y soporte antivirus máquinas en colocación // 3.1 Colocación (Incluye Licenciamiento) // 3.2 DRP hosting // 3.3 Servicios Administrados SO y BD // 3.4 Replicacion DC // 3.5 Cross Conexiones terceros // 3.6 Licenciamiento, Administración y soporte antivirus maquinas Hosting //4.1.1 Licenciamiento de Plataformas de Seguridad // 4.1.2 Servicios de Seguridad CSOC // 4.1.3 Administración de Plataformas de Seguridad de Usuarios, Web y BD // 5.1.1 Servicio de gestión y administración de conectividad LAN/WLAN en sede // 5.1.2 Solución integral de conectividad Línea de Emergencia Vida 103 // 5.1.3 Servicio de NOC

Nota 1: En atención a que todas las líneas de servicio quedan activas mediante la suscripción de la presente acta; es necesario mes a mes desde el informe de supervisión verificar la prestación efectiva (Nula / Parcial / Total) de cada uno de los servicios contenidos en ellas.

En el marco de las condiciones para iniciar la ejecución del contrato de conformidad con lo establecido en las obligaciones específicas del contrato numeral 1, se relacionan los siguientes anexos:

1. Registro Presupuestal No. 497426 del 05 de junio de 2026
2. Plan de trabajo
3. Cronograma de activación de servicios

En constancia de lo anterior, se suscribe la presente acta de inicio el día martes, 30 de junio de 2026, en la ciudad de Bogotá D.C.

Por el contratista

Firmado digitalmente por Monica Nova Peña

MÓNICA VIVIANA NOVA PEÑA
C.C. **1.018.426.005**
Representante Legal
UT SERVICIOS TECNOLÓGICOS SSC

Por el Supervisor

Firmado digitalmente por Javier Francisco Rodriguez Moreno

JAVIER FRANCISCO RODRÍGUEZ MORENO
C.C. CC. 80000431
Jefe de la Oficina de Tecnologías y Sistemas de Información – OTSI (E)

	Nombre	Firma	Fecha
Proyectó	Luis Henan Castellanos - Contratista - OTSI	Firmado digitalmente por Luis Hernan Castellanos G.	30/06/2026
Reviso	Guillermo Antonio Rengifo - Contratista - OTSI Oscar Andrés Casas - Contratista - OTSI John Anderson Hernández Correa - Contratista - OTSI	Firmado digitalmente por Oscar Casas Firmado digitalmente por GUILLERMO ANTONIO RENGIFO BUITRAGO John Anderson Hernández Correa	30/06/2026
Aprobó	Javier Francisco Rodríguez Moreno - Jefe Oficina de Tecnologías y Sistemas de Información (E)	Firmado digitalmente por Javier Francisco Rodriguez Moreno	30/06/2026
Los arribas firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad, lo presentamos para firma.			

Notas:
NOTA 1: *El objeto del contrato no es susceptible de modificación.*
NOTA 2: *El presente Formato contiene la información básica que debe contener una solicitud de modificación. Lo anterior sin perjuicio de la información y soportes adicionales que se deban relacionar atendiendo la naturaleza del contrato o convenio o el tipo de modificación y la complejidad de esta.*

Archívese en Expediente contractual Incluir número - vigencia

VERSIÓN INCIAL	DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO	FECHA	VERSIÓN FINAL
2	Se modifica el formato de Acta de Inicio, para dar cumplimiento a la “Resolución 1366 de 2020 "Por medio de la cual se adoptan los procesos del MIPG - SIG de la Unidad Nacional de Protección, El Manual Institucional de Política de Servicio al Ciudadano, el Manual para la Formulación y Seguimiento de Planes, el Manual de Gestión de Indicadores, el Manual de Gestión Estratégica Integrada de Gestión de Riesgo y se derogan las Resoluciones Nos, 1820 de 2018 y 1565 del 2019"	20/08/2021	3
3	Se modifica el formato de Acta de Inicio en forma y orden de contenido y se ajustan los logos de acuerdo con la imagen institucional	04/09/2025	4
4	Se corrige reglón de firmas, cambiando por el jefe de dependencia a por el contratista.	08/10/2025	5

SGT-UNP-UT-SSC 2026 001

Bogotá, 30 de junio de 2026

Señores
UNIDAD NACIONAL DE PROTECCIÓN-UNP
Atn. Javier Francisco Rodríguez Moreno.
Jefe (E) Oficina de Tecnología y Sistemas de Información - OTSI
francisco.moreno@unp.gov.co
Teléfono: 601 4269800
Calle 20ª # 44 - 41 Puente Aranda
Bogotá, Colombia

Ref.: **Contrato No. CPS - 2546 - 2026 cuyo objeto es "CONTRATAR LA GESTIÓN INTEGRAL DE LOS SERVICIOS TECNOLÓGICOS DE LA UNP".**

Asunto: **Documentos Acta de Inicio de la UT Servicios Tecnológicos SSC – Cto 2546 de 2026.**

Respetados señores,

En calidad de adjudicatarios del **Contrato 2546 de 2026**, y como parte del compromiso con el proceso de activación y formalización del contrato, nos permitimos compartir el enlace donde encontrarán la **documentación preliminar clave** para su revisión anticipada, previo a la ceremonia de firma del acta de inicio.

Este espacio digital contiene los insumos fundamentales que permitirán facilitar el análisis técnico y operativo por parte de la UNP, y garantizar una sesión de inicio ágil, estructurada y alineada con los compromisos contractuales.

A continuación, detallamos los documentos disponibles en el repositorio:

Plan de trabajo
Cronograma de activación de servicio

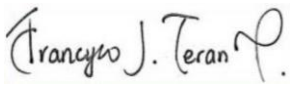
Acceso a la información preliminar:

Documentación para acta de inicio

Esta entrega se realiza a título informativo, en calidad de adjudicatarios, y con el objetivo de garantizar una revisión técnica anticipada de los aspectos fundamentales del inicio del proyecto.

Quedamos atentos a cualquier comentario o solicitud adicional que la supervisión considere pertinente frente a esta documentación.

Cordialmente,



Francisco José Terán Mosquera
Gerente de Proyecto
UT Servicios Integrales SSC 2026

Elaboró: Brenda Sabogal
Gestor Documental

Aprobó: Patricia Alvarez
Líder de Proyecto PMO

Unión Temporal Servicios Tecnológicos SSC

PLAN DE TRABAJO

Contrato 2546 - 2026

UNIDAD NACIONAL DE PROTECCIÓN UNP

FECHA DE ELABORACIÓN: 30/06/2026

Tabla de Contenido

1 Información general del plan de activación 5
1.1 Descripción general del contrato 5
1.2 Objetivo del plan de activación 5
1.3 Estructura operacional 5
1.4 Cronograma de activación del servicio 6
2 Plan de Transición del Servicio 7
3 Activación del servicio 7
3.1 Activación al servicio de mesa de servicios 7
3.1.1 Introducción al Servicio de Mesa: 7
3.1.2 Estructura Operativa y Roles: 8
3.1.3 Proceso de Activación mesa de servicios: 8
3.1.4 Assumptions, Condiciones y Prerrequisitos: 8
3.2 Introducción a la Gestión de Servicios (ITIL): 9
3.2.1 Estructura Operativa y Roles: 9
3.2.2 Proceso de Activación: 10
3.2.3 Consideraciones Técnicas y Operativas: 10
3.2.4 Assumptions, Condiciones y Prerrequisitos: 10
3.3 Activación de línea de servicios centrales 11
3.3.1 Introducción al Servicio 11
3.3.2 Estructura Operativa y Roles 11
3.3.3 Proceso de Activación 11
3.3.4 Assumptions, Condiciones y Prerrequisitos: 12
3.4 Activación de Recuperación de desastres DRP - Datacenter alterno 12
3.4.1 Introducción al Servicio: 12

3.4.2 Proceso de Activación 12
3.4.3 Consideraciones Técnicas y Operativas 13
3.4.4 Assumptions, Condiciones y Prerrequisitos 13
3.5 Activación de soporte especializado plataformas centrales 13
3.5.1 Introducción al Servicio de seguridad de la información: 13
3.5.2 Estructura Operativa y Roles: 13
3.5.3 Proceso de Activación: 14
3.5.4 Consideraciones Técnicas y Operativas: 15
3.5.5 Assumptions, Condiciones y Prerrequisitos: 15
3.5.6 Acceso a Credenciales de Dominio y Sistemas Críticos: 15
3.5.7 Documentación Técnica y Configuraciones Actuales: 16
3.5.8 Coordinación de Recursos y Comunicación: 16
3.6 Activación de línea de servicios en sede - Conectividad LAN y WLAN 16
3.6.1 Introducción al Servicio 16
3.6.2 Estructura Operativa y Roles 16
3.6.3 Proceso de Activación: 17
3.6.4 Consideraciones Técnicas y Operativas: 17
3.6.5 Assumptions, Condiciones y Prerrequisitos 18
3.6.6 Dimensionamiento del Equipo de Trabajo: 18
4 Gestión de Riesgos durante la Activación: 18
4.1 Estrategia de mitigación durante la transición 19
4.2 Plan de trabajo de transición 19
4.3 Seguimiento y control 20
5 Estrategia de Comunicación durante la Activación: 20
6 Responsabilidades asociadas a la gestión de activos de TI: 21
6.1 Metodología de Gestión de Activos de TI 21
6.2 Consulta y Actualización de Información 21

6.3 Generación de Reportes 21
6.4 Control de Fechas de Mantenimiento y Expiración de Garantías 21
6.5 Administración de la CMDB 21
6.6 Responsabilidades del Contratista 22
7 Anexos 22
8 Cuadro de aprobación. 22

1 Información general del plan de Trabajo

1.1 Descripción general del contrato

El contrato No. 2546 de 2026, suscrito entre la Unidad Nacional de Protección (UNP) y la Unión Temporal Servicios Tecnológicos SSC, tiene como objeto la gestión integral de los servicios tecnológicos de la UNP. Este contrato incluye la provisión de una solución integral en modalidad de servicio, abarcando componentes de tecnología, soporte informático, telefonía, y telecomunicaciones para los recursos existentes de la UNP, así como la gerencia de los proyectos tecnológicos necesarios para asegurar una prestación de servicios eficiente y de alta calidad.

1.2 Objetivo del plan de activación

El objetivo del Plan de Activación es asegurar la implementación efectiva de los servicios tecnológicos contratados por la Unidad Nacional de Protección (UNP) bajo el contrato No. 2546 de 2026. Estableciendo un conjunto de actividades, responsables, entregables y tiempos necesarios para la activación progresiva de los servicios de TI en la UNP, garantizando la continuidad del servicio, cumplimiento de ANS y alineación con ITIL 4.

1.3 Estructura operacional

La Unión Temporal Servicios Tecnológicos SSC utilizará la siguiente estructura, para respaldar el proceso de comunicaciones, con el objetivo de lograr una coordinación efectiva de la comunicación abierta entre las partes involucradas.

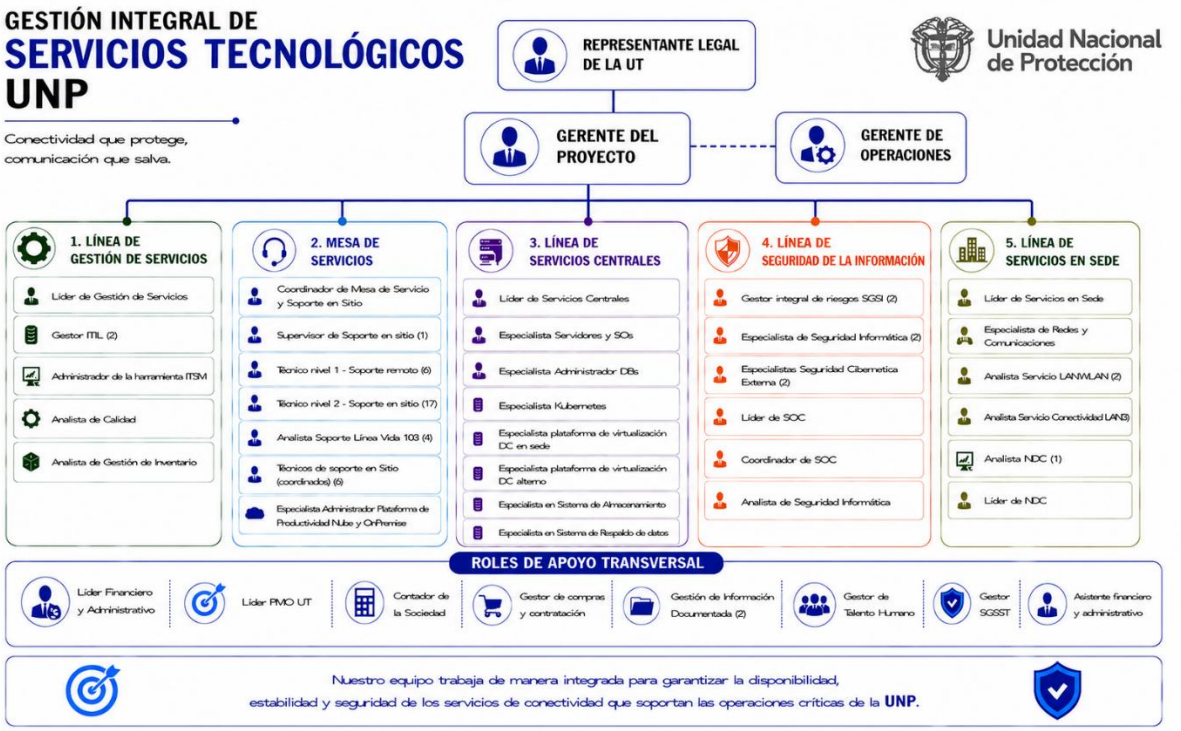


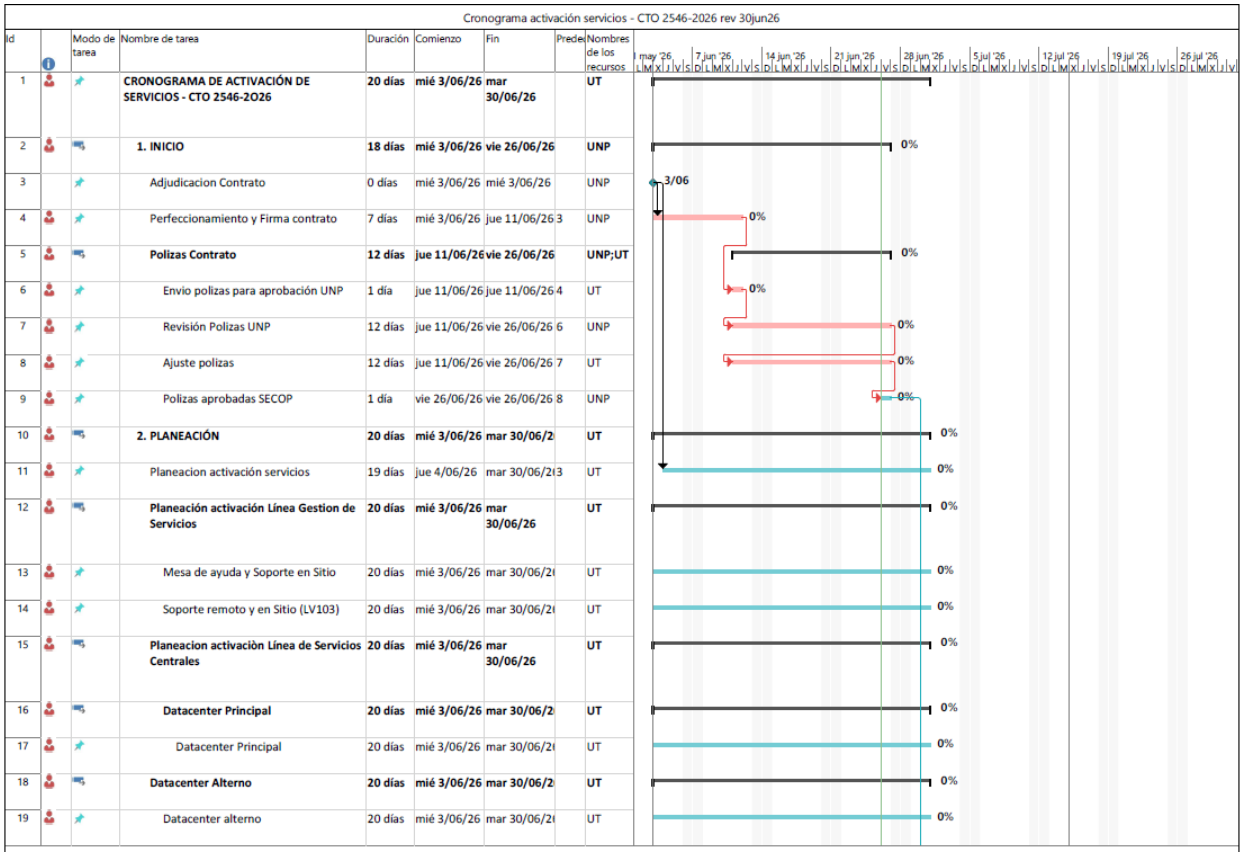
Imagen 1. Organigrama. Fuente: Propia

1.4 Cronograma de activación del servicio

El cronograma de activación es una herramienta clave para la planificación y seguimiento de todas las actividades relacionadas con la implementación de los servicios en el marco del contrato con la Unidad Nacional de Protección (UNP). Este cronograma proporciona una visión general de las etapas críticas, los hitos clave y los plazos establecidos para la activación de cada línea de servicio, asegurando que todas las tareas se completen de manera oportuna y coordinada.

En esta sección, se presenta una captura del cronograma de activación, que ofrece una visualización rápida de las fases y actividades principales. El cronograma completo, que incluye todos los detalles específicos, se encuentra disponible como anexo en formato Microsoft Project. Este archivo detallado permite una gestión dinámica del proyecto, facilitando la actualización, revisión y ajuste de los plazos y recursos a medida que avanza la ejecución del contrato.

Este enfoque asegura que todas las partes interesadas tengan acceso a una herramienta integral de planificación, que respalde la entrega exitosa de los servicios según los términos acordados.



Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predec	Nombres de los recursos
1		**CRONOGRAMA DE ACTIVACIÓN DE SERVICIOS - CTO 2546-2026**	**20 días**	**mié 3/06/26**	**mar 30/06/26**		**UT**
2		**1. INICIO**	**18 días**	**mié 3/06/26**	**vie 26/06/26**		**UNP**
3		Adjudicacion Contrato	0 días	mié 3/06/26	mié 3/06/26		UNP
4		Perfeccionamiento y Firma contrato	7 días	mié 3/06/26	jue 11/06/26	3	UNP
5		**Polizas Contrato**	**12 días**	**jue 11/06/26**	**vie 26/06/26**		**UNP;UT**
6		Envio polizas para aprobación UNP	1 día	jue 11/06/26	jue 11/06/26	4	UT
7		Revisión Polizas UNP	12 días	jue 11/06/26	vie 26/06/26	6	UNP
8		Ajuste polizas	12 días	jue 11/06/26	vie 26/06/26	7	UT
9		Polizas aprobadas SECOP	1 día	vie 26/06/26	vie 26/06/26	8	UNP
10		**2. PLANEACIÓN**	**20 días**	**mié 3/06/26**	**mar 30/06/2**		**UT**
11		Planeacion activación servicios	19 días	jue 4/06/26	mar 30/06/2	3	UT
12		**Planeación activación Línea Gestion de Servicios**	**20 días**	**mié 3/06/26**	**mar 30/06/26**		**UT**
13		Mesa de ayuda y Soporte en Sitio	20 días	mié 3/06/26	mar 30/06/2		UT
14		Soporte remoto y en Sitio (LV103)	20 días	mié 3/06/26	mar 30/06/2		UT
15		**Planeacion activaciòn Línea de Servicios Centrales**	**20 días**	**mié 3/06/26**	**mar 30/06/26**		**UT**
16		**Datacenter Principal**	**20 días**	**mié 3/06/26**	**mar 30/06/2**		**UT**
17		Datacenter Principal	20 días	mié 3/06/26	mar 30/06/2		UT
18		**Datacenter Alterno**	**20 días**	**mié 3/06/26**	**mar 30/06/2**		**UT**
19		Datacenter alterno	20 días	mié 3/06/26	mar 30/06/2		UT

Ilustración 1 Cronograma de Activación

Imagen 2. Captura del cronograma de activación de servicio Fuente: Propia

2 Plan de Transición del Servicio

Durante la fase de activación y transición de los servicios, se llevarán a cabo las actividades necesarias para la construcción, validación, despliegue y puesta en operación de los servicios tecnológicos, garantizando su adecuada estabilización, continuidad y cumplimiento de los Acuerdos de Nivel de Servicio (ANS) definidos por la Entidad. Este proceso incluye la transferencia del conocimiento necesario hacia la fase de operación, asegurando que los servicios puedan ser gestionados de manera eficiente dentro de los niveles de servicio acordados.

Para garantizar el éxito de la transición, los servicios serán introducidos de manera controlada, progresiva y no disruptiva, asegurando que aporten el valor esperado a la operación de la Entidad desde su entrada en funcionamiento.

Durante esta fase, se adelantará un proceso integral de recepción, validación y alistamiento de los servicios existentes, incluyendo infraestructura, plataformas, redes, servicios en sede y herramientas de gestión (ITSM – IVANTI), con el fin de establecer su estado actual e identificar brechas, riesgos y necesidades de ajuste para una adecuada entrada en operación.

En este contexto, la activación de los servicios contempla las siguientes actividades principales:

- Recepción y verificación de los servicios TIC actuales, asegurando que todos los servicios, activos tecnológicos e infraestructura asociada sean recibidos en las condiciones técnicas y operativas establecidas.
- Medición y calibración de los Acuerdos de Nivel de Servicio (ANS), mediante la evaluación de los indicadores existentes y su ajuste para alinearlos con las expectativas y niveles requeridos por la UNP.
- Configuración y alistamiento de la herramienta de gestión de servicios (IVANTI), incluyendo la parametrización de flujos, servicios, CMDB y mecanismos de control, en alineación con prácticas ITIL v4.
- Validación técnica y funcional de los servicios, a través de pruebas de disponibilidad, conectividad y desempeño que permitan asegurar su correcta operación.
- Verificación de mecanismos de monitoreo, respaldo y continuidad, incluyendo la articulación con el datacenter alterno.
- Capacitación y transferencia de conocimiento, dirigida a los equipos operativos, para garantizar el uso adecuado de herramientas, procesos y prácticas implementadas.

Como resultado, se dispondrá de un entorno de servicios estabilizado, validado y documentado, listo para su entrada formal a la fase de operación, bajo un esquema controlado, alineado con ITIL v4 y orientado a la mejora continua.

3 Activación del servicio

3.1 Activación al servicio de mesa de servicios

3.1.1 Introducción al Servicio de Mesa:

El Servicio de Mesa de Niveles 1 y 2 en la Unidad Nacional de Protección (UNP) está diseñado para ser el primer punto de contacto entre los usuarios de la entidad y el equipo de tecnología de la información.

Su función principal es resolver incidentes y gestionar solicitudes de servicio que no requieran una intervención técnica profunda. El objetivo es maximizar la eficiencia operativa y la satisfacción del usuario final al garantizar una rápida resolución de problemas y un acceso fácil a los servicios necesarios.

3.1.2 Estructura Operativa y Roles:

- **Coordinador de mesa de servicio y soporte en sitio**: Coordina todas las operaciones del servicio de mesa, incluida la gestión del personal, la planificación estratégica y la calidad del servicio.
- **Supervisor de soporte en sitio**: Supervisar las actividades relacionadas al personal técnicos de Nivel 2, garantizando la calidad del servicio y atención.
- **Técnicos de Nivel 1**: Son el primer punto de contacto. Resuelven incidentes básicos y gestionan las solicitudes de los usuarios. Si un incidente no se puede resolver en este nivel, se escala al Nivel 2.
- **Técnicos de Nivel 2**: Manejan incidentes y problemas más complejos que requieren un conocimiento técnico detallado o acceso a configuraciones más profundas del sistema.

3.1.3 Proceso de Activación mesa de servicios:

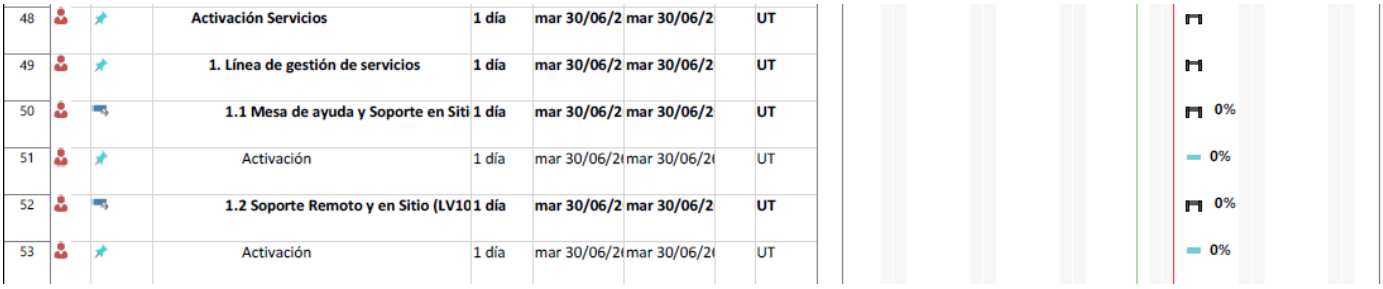


Ilustración 2 Activación Mesa de Servicios

- El proceso de activación de la Mesa de Servicios en la UNP comienza con la configuración inicial de la infraestructura física de la mesa de servicio tales como puestos de trabajo y red.
- Realizar un diagnóstico inicial de la herramienta IVANTI, evaluando su configuración, funcionalidades activas, estado de la CMDB, flujos de atención y alineación con ITIL 4, con el fin de identificar brechas y definir acciones de mejora para su puesta a punto
- Una vez configurada, la infraestructura se pone en marcha, con técnicos de Nivel 1 y Nivel 2 responsables de operar el sistema y gestionar los incidentes según su complejidad. Los protocolos de escalamiento están claramente establecidos para asegurar que cualquier incidente que no pueda ser resuelto internamente sea rápidamente escalado a un equipo de soporte externo o a especialistas más capacitados. Este proceso no solo busca minimizar el tiempo de inactividad sino también maximizar la productividad y eficiencia operativa a través de una rápida resolución de problemas, todo mientras mantiene a todas las partes informadas sobre el progreso de los incidentes escalados.

3.1.4 Assumptions, Condiciones y Prerrequisitos:

- **Asumptions**: El personal tiene las competencias técnicas requeridas y acceso a las herramientas necesarias para ejecutar sus funciones eficazmente.
- **Condiciones**: La infraestructura de IT de la UNP debe estar en condiciones operativas óptimas para soportar la implementación y operación continua del servicio de mesa.
- **Prerrequisitos:** Antes de la activación, debe asegurarse los siguientes prerrequisitos:

- ✓ **Infraestructura física:** Adaptación de los espacios laborales para la mesa de servicio y validación de las condiciones ergonómicas por parte del área de Seguridad y Salud en el trabajo de la Unión Temporal.
- ✓ **Infraestructura de Red**: Asegurar una conexión de red estable y segura con capacidad adecuada para soportar todas las operaciones de la Mesa de Servicios.
- ✓ **Software de Gestión de Tickets**: Acceso al sistema de gestión de tickets (ITSM Ivanti), que soporte la captura, seguimiento y resolución de incidentes y solicitudes.
- ✓ **Sistemas Telefónicos**: Sistemas de telefonía confiables y adecuados que permitan la medición del 100% de indicadores telefónicos.
- ✓ **Acceso a Sistemas y Aplicaciones**: Accesos configurados y probados a todos los sistemas críticos y aplicaciones necesarias para el soporte técnico.
- ✓ **Herramientas de Diagnóstico y Resolución**: Disponibilidad de herramientas de software para diagnóstico remoto y resolución de problemas (Ivanti).
- ✓ **Protocolos de Seguridad**: Entrega de protocolos de seguridad para proteger los datos y la información del usuario y de la empresa.
- ✓ **Acceso a la documentación técnica**: Asegurar que el personal tenga fácil acceso a la documentación técnica necesaria para los equipos y software que soportan.
- ✓ **Monitoreo y Reporte de Incidentes**: Sistemas para el monitoreo y reporte continuo de incidentes para evaluar la efectividad del servicio de mesa.
- ✓ **Herramientas de Colaboración**: Implementación de herramientas de colaboración para permitir una comunicación eficiente entre los miembros del equipo y otros departamentos.
- ✓ **Gestión de Cambios**: Procesos establecidos para la gestión de cambios en el entorno IT que puedan afectar los servicios que ofrece la mesa.
- ✓ **Asignación de carnets y accesos permanente a las oficinas de la UNP.**
- ✓ **Asignación de parqueadero motos para analistas de mesa y soporte en sitio que estarán en las instalaciones de la UNP.**

Esto garantizará que el Servicio de Mesa de Niveles 1 y 2 esté preparado para operar eficientemente desde el primer día, con una clara delineación de roles y procesos, y con la infraestructura y entrenamiento adecuados para soportar sus operaciones.

3.2 Introducción a la Gestión de Servicios (ITIL):

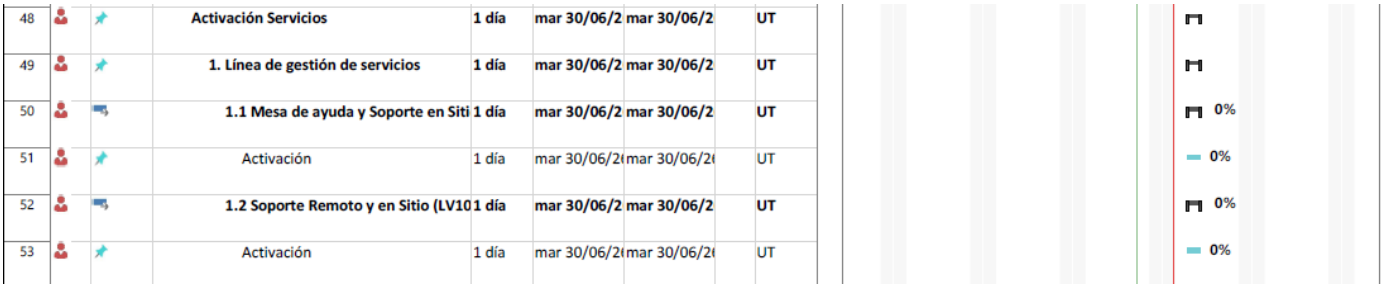
○ La implementación de la Gestión de Servicios ITIL en la UNP se orienta a estandarizar los procesos y mejorar la eficiencia y efectividad del servicio IT en 12 prácticas definidas en el contrato, las cuales son: Gestión de la implementación, incidentes, solicitudes de servicios, problemas, activos TI, habilitación del cambio, gestión de niveles de servicio, disponibilidad y catálogo de servicios.

○ ITIL, siendo un conjunto de prácticas para la gestión de servicios de TI, ayudará a la UNP a alinear los servicios IT con las necesidades de la organización, mejorando la gestión de recursos, la entrega de servicios y la satisfacción del cliente.

3.2.1 Estructura Operativa y Roles:

○ La estructura operativa para la Gestión de Servicios ITIL en la UNP se establece con roles claramente definidos:
○ **Líder línea de gestión del servicio**: Responsable de la supervisión general y la implementación de las prácticas de ITIL dentro de la organización.
○ **Gestores ITIL 4**: Cada proceso ITIL (como gestión de incidentes, problemas y cambios) es gestionado por un propietario de proceso que asegura la ejecución efectiva y eficiente de su área respectiva.

3.2.2 Proceso de Activación:



48		Activación Servicios	1 día	mar 30/06/2	mar 30/06/2	UT
49		1. Línea de gestión de servicios	1 día	mar 30/06/2	mar 30/06/2	UT
50		1.1 Mesa de ayuda y Soporte en Siti	1 día	mar 30/06/2	mar 30/06/2	UT
51		Activación	1 día	mar 30/06/2	mar 30/06/2	UT
52		1.2 Soporte Remoto y en Sitio (LV10	1 día	mar 30/06/2	mar 30/06/2	UT
53		Activación	1 día	mar 30/06/2	mar 30/06/2	UT

Ilustración 3 Activación Gestión de Servicios

- El proceso de activación de la Gestión de Servicios ITIL en la UNP abarca varias etapas clave diseñadas para asegurar que los principios ITIL se implementen de manera efectiva y sostenible:
- **Planificación y Diseño**: Se elabora un plan exhaustivo que detalla las prácticas específicas de ITIL a implementar, adaptadas a las necesidades y objetivos de la UNP. Este plan no solo selecciona las prácticas relevantes, sino que también establece los marcos temporales y recursos necesarios para su ejecución.
- **Divulgación y Refuerzo de la Cultura ITIL**: Para fomentar una adopción generalizada y mejorar la adherencia a las prácticas de ITIL, se implementa una estrategia de divulgación centrada en la educación y el refuerzo continuo de la cultura ITIL. Esta estrategia incluye:

  - ✓ **Sesiones de Sensibilización**: Organizar sesiones regulares de sensibilización para todo el personal, no solo para aquellos directamente involucrados en ITIL, para explicar los beneficios y la importancia de seguir las prácticas de ITIL.
  - ✓ **Materiales Educativos**: Distribución de materiales educativos que resaltan los principios de ITIL, historias de éxito y estudios de caso que demuestren el impacto positivo de ITIL en organizaciones similares.

- Estas actividades no solo promueven una mejor comprensión y aceptación de ITIL dentro de la organización, sino que también fortalecen el compromiso con la mejora continua de los procesos de gestión de servicios, asegurando que ITIL se convierta en una parte integral de la cultura organizativa de la UNP.

3.2.3 Consideraciones Técnicas y Operativas:

Las consideraciones técnicas incluyen la parametrización de sistemas de software para la automatización de procesos ITIL (ITSM), como herramientas de gestión de incidentes y de cambios. Además, es crucial mantener una comunicación efectiva entre todos los niveles de la organización para asegurar la adopción y eficacia de los procesos ITIL.

3.2.4 Assumptions, Condiciones y Prerrequisitos:

- **Assumptions**: Se asume que el personal de la UNP está comprometido y dispuesto a adoptar nuevas prácticas y que existen suficientes recursos para la implementación efectiva de ITIL.
- **Condiciones**: La infraestructura de IT y las plataformas de software deben estar actualizadas y ser capaces de soportar la metodología ITIL.

- **Prerrequisitos**:

  - ✓ Las herramientas de software necesarias para los procesos deben estar plenamente operativas.
  - ✓ Para garantizar una gestión efectiva de la gestión de la disponibilidad de los servicios de antivirus, red, internet, data center y colocación, por ejemplo, se debe contar con herramientas de monitoreo capaces de medir KPIs críticos para cada servicio. Estas herramientas permiten a la UNP monitorizar el rendimiento, identificar y resolver problemas de manera proactiva, y optimizar continuamente los servicios IT.
  - ✓ **Soporte Ejecutivo y Compromiso Organizacional**: Apoyo firme de la alta dirección para la implementación de ITIL, proporcionando los recursos necesarios y promoviendo una cultura de gestión de servicios en toda la organización.
  - ✓ **Programa de Comunicación**: Desarrollo de un programa de comunicación para informar y educar a todos los usuarios sobre los procesos de ITIL, los beneficios esperados y cómo interactuar con el nuevo sistema de gestión de servicios.

3.3 Activación de línea de servicios centrales

3.3.1 Introducción al Servicio

El servicio de línea de servicios centrales está diseñado para asegurar la operación continua y eficiente de la infraestructura tecnológica de la Unidad Nacional de Protección. Este servicio incluye la administración de servidores, sistemas operativos, bases de datos, y el soporte técnico necesario para garantizar el rendimiento óptimo de las plataformas críticas.

3.3.2 Estructura Operativa y Roles

Líder de Servicios Centrales: Responsable de la supervisión general del servicio, coordinando la operación del datacenter alterno, la ejecución de planes de recuperación ante desastres (DRP) y asegurando el cumplimiento de los tiempos de recuperación (RTO/RPO). Gestiona la articulación entre los equipos técnicos y actúa como punto de contacto con la Entidad para la continuidad del servicio.

Especialistas de Sistemas Operativos: Responsables de la administración, configuración y soporte de los sistemas operativos en el datacenter alterno. Garantizan la disponibilidad y correcta operación de los servidores durante escenarios de contingencia, ejecutan procedimientos de recuperación y validan la consistencia de los entornos replicados.

Especialistas de Bases de Datos: Encargados de la administración y recuperación de las bases de datos replicadas hacia el datacenter alterno. Validan la integridad, sincronización y disponibilidad de la información, asegurando la continuidad de los servicios críticos y el cumplimiento del RPO definido.

Especialistas de Virtualización: Responsables de la gestión de las plataformas de virtualización, incluyendo la configuración de clústeres, replicación de máquinas virtuales y ejecución de procesos de conmutación (failover y failback). Garantizan la disponibilidad de los entornos virtuales en el sitio alterno.

Especialistas de Backup y Storage: Encargados de la gestión de los sistemas de respaldo y almacenamiento, asegurando la correcta ejecución de copias de seguridad, la integridad de los datos y la disponibilidad de la información para procesos de recuperación. Apoyan la restauración de servicios en el datacenter alterno y validan la coherencia de los datos recuperados.

3.3.3 Proceso de Activación

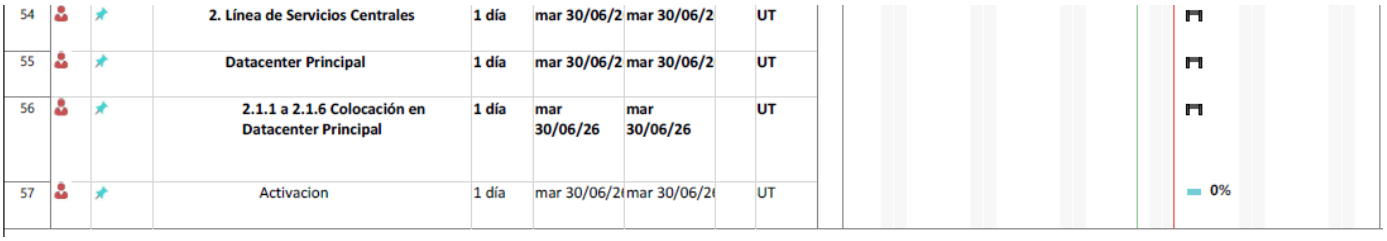


Ilustración 4 Activación de Servicios Centrales (Datacenter)

- Recibir formalmente la infraestructura tecnológica del Data Center.
- Realizar el assessment de la infraestructura tecnológica contemplada dentro del contrato
- Revisar configuraciones de virtualización y almacenamiento.
- Identificar servicios y aplicaciones alojadas en la infraestructura.
- Verificar capacidades instaladas y uso de recursos.
- Documentar la arquitectura actual de plataformas.
- Pruebas de Operación: Validación de conectividad y disponibilidad de servicios.

3.3.4 Assumptions, Condiciones y Prerrequisitos:

Todos los accesos necesarios (físicos y lógicos) serán proporcionados al equipo de UT Servicios Tecnológicos.

3.4 Activación de Recuperación de desastres DRP - Datacenter alterno

3.4.1 Introducción al Servicio:

El servicio de Recuperación de Desastres (DRP) en el Datacenter alterno está diseñado para garantizar la continuidad del negocio en caso de un evento que afecte la operación del Data Center principal. Este servicio incluye la replicación de datos, la activación de sistemas de respaldo y la ejecución de planes de contingencia

3.4.2 Proceso de Activación

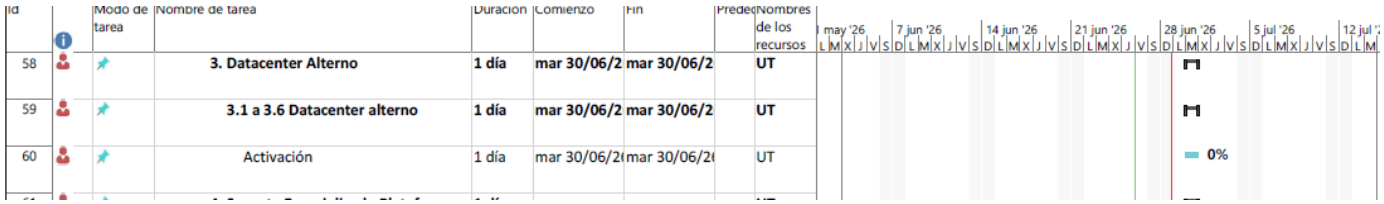


Ilustración 5 Activación de Servicios Centrales (Datacenter Alterno)

- Se realizará la identificación de la infraestructura disponible como sitio de datacenter alterno, con el fin de establecer su alcance, componentes y capacidad de soporte frente a escenarios de contingencia.
- Posteriormente, se llevará a cabo la validación de la configuración y del estado operativo del sitio alterno, evaluando su disponibilidad, funcionamiento y nivel de preparación para asumir la operación de los servicios.

- Se verificará la conectividad entre el datacenter principal y el datacenter alterno, asegurando la correcta comunicación entre ambos entornos y la continuidad en la transferencia de datos.
- Asimismo, se identificarán y validarán los mecanismos de replicación de la información, analizando su tipo, frecuencia y consistencia, con el propósito de garantizar la integridad de los datos.
- Se determinarán los servicios críticos que cuentan con respaldo en el sitio alterno, estableciendo su nivel de cobertura frente a escenarios de falla del datacenter principal.
- De igual manera, se realizará la revisión de los planes de recuperación ante desastres (DRP), verificando su existencia, actualización y aplicabilidad operativa.
- Finalmente, se validarán los tiempos de recuperación definidos, incluyendo el Tiempo Objetivo de Recuperación (RTO) y el Punto Objetivo de Recuperación (RPO), con el fin de asegurar que se ajusten a los requerimientos del servicio y a los niveles de disponibilidad esperados.

3.4.3 Consideraciones Técnicas y Operativas

- La replicación de datos debe garantizar un RTO y RPO de 2 horas o menos.
- La infraestructura del Datacenter alterno debe estar preparada para soportar un incremento de carga del 50% sobre la operación normal.

3.4.4 Assumptions, Condiciones y Prerrequisitos

- Se confirma que el Datacenter alterno cumple con las certificaciones TIER II o ICREA Nivel III.
- Se requiere acceso total a los sistemas y datos críticos para la implementación del DRP.

3.5 Activación de soporte especializado plataformas centrales

3.5.1 Introducción al Servicio de seguridad de la información:

En el entorno digital actual, donde las amenazas cibernéticas evolucionan constantemente, la protección de la infraestructura tecnológica de una entidad es de máxima prioridad. Este documento describe la implementación de un servicio integral de seguridad informática centralizada en el Datacenter principal de la entidad es necesario para asegurar la continuidad y la integridad de los servicios esenciales.

3.5.2 Estructura Operativa y Roles:

La prestación del servicio de seguridad informática está diseñada para asegurar la protección integral de la infraestructura tecnológica de la entidad. Esto se logra mediante una estructura operativa que se enfoca en dos roles clave, cada uno especializado en áreas críticas de la seguridad informática:

- Lider de SOC
- Coordinador del SOC
- Lider de Seguiridad de la Información
- Gestor Integral de Riesgos
- Analista de >Seguridad Informática
- Especialistas Seguridad Cibernetica Externa
- Especialista en seguridad informática

Especialista de Seguridad Informática Fortinet: Este profesional es responsable de la administración, configuración y optimización de las soluciones de seguridad de Fortinet incluidas en el contrato. Sus funciones principales incluyen:

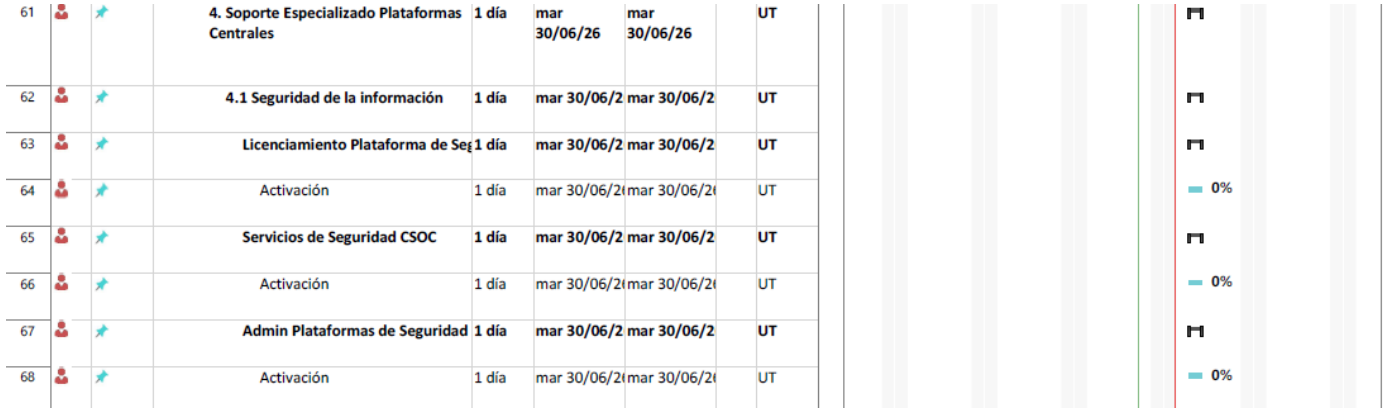
- ✓ Manejo de FortiEDR: Implementación y gestión de la solución de Endpoint Detection and Response (EDR) de Fortinet, garantizando la protección avanzada contra amenazas y la capacidad de respuesta automatizada a incidentes en los endpoints.
- ✓ Gestión de FortiSIEM: Configuración y operación del sistema de Security Information and Event Management (SIEM), que centraliza el monitoreo y análisis de eventos de seguridad, permitiendo una detección temprana de amenazas y una respuesta rápida.
- ✓ Administración de FortiSandbox: Manejo de la solución de sandboxing, que analiza archivos sospechosos en un entorno seguro para identificar posibles amenazas antes de que ingresen a la red corporativa.
- ✓ Gestión de FortiWAF: Configuración y supervisión del firewall de aplicaciones web (WAF), protegiendo las aplicaciones web de la entidad contra vulnerabilidades y ataques.
- ✓ Plataforma de reporte de eventos: Elaboración de informes detallados sobre los eventos de seguridad detectados y gestionados a través de las plataformas, proporcionando información valiosa para la toma de decisiones estratégicas en seguridad.

Especialista de Seguridad Informática Palo Alto: Este especialista se dedica a la administración y configuración de los dispositivos de seguridad de Palo Alto Networks que utiliza la entidad. Sus responsabilidades incluyen:

- ✓ Configuración de Dispositivos Palo Alto: Implementación y ajuste de las políticas de seguridad en los firewalls de próxima generación (NGFW) de Palo Alto, asegurando que las reglas de seguridad estén alineadas con las necesidades y riesgos específicos de la entidad.
- ✓ Gestión de la Seguridad en la Red: Supervisión del tráfico de red, aplicación de medidas de prevención de amenazas y optimización del rendimiento de los dispositivos Palo Alto para garantizar una protección eficaz y continua.
- ✓ Integración con Otras Plataformas: Coordinación de la integración de los dispositivos Palo Alto con otras soluciones de seguridad implementadas en la entidad, como el SIEM, para crear un ecosistema de seguridad cohesivo y eficiente.
- ✓ Estos roles trabajan de manera coordinada para garantizar que todos los aspectos de la seguridad informática de la UNP estén cubiertos, proporcionando una defensa robusta y adaptable frente a las amenazas cibernéticas. La colaboración entre los especialistas asegura una respuesta integral y eficaz a los incidentes, además de contribuir a la mejora continua de la postura de seguridad de la entidad.

3.5.3 Proceso de Activación:

A partir de la firma del acta de inicio, el servicio de seguridad informática se considera formalmente activo, lo que significa que los especialistas asignados están disponibles de inmediato para atender cualquier consulta, reunión o necesidad específica que surja en la UNP. Estos especialistas, con su amplio conocimiento y experiencia, brindarán apoyo en todas las actividades necesarias para garantizar la seguridad y protección de la infraestructura de la entidad.



61		4. Soporte Especializado Plataformas Centrales	1 día	mar 30/06/26	mar 30/06/26	UT
62		4.1 Seguridad de la información	1 día	mar 30/06/2	mar 30/06/2	UT
63		Licenciamiento Plataforma de Se	1 día	mar 30/06/2	mar 30/06/2	UT
64		Activación	1 día	mar 30/06/2	mar 30/06/2	UT
65		Servicios de Seguridad CSOC	1 día	mar 30/06/2	mar 30/06/2	UT
66		Activación	1 día	mar 30/06/2	mar 30/06/2	UT
67		Admin Plataformas de Seguridad	1 día	mar 30/06/2	mar 30/06/2	UT
68		Activación	1 día	mar 30/06/2	mar 30/06/2	UT

Ilustración 6 Activación de Plataformas Centrales y Seguridad de la Información

- Durante la fase de transición, se realizará la activación de las plataformas centrales mediante la recepción y análisis de la información técnica de servidores físicos y virtuales, identificando su configuración, servicios asociados y estado actual.
- Se validará el funcionamiento de las plataformas, evaluando disponibilidad, consumo de recursos y desempeño general, así como las configuraciones de virtualización y almacenamiento. Adicionalmente, se verificará la operación de los servicios base y las aplicaciones alojadas, asegurando su correcta interdependencia.
- De igual forma, se integrarán las plataformas al esquema de monitoreo y a la herramienta ITSM (IVANTI), configurando alertas y eventos para la gestión operativa. Se validarán los mecanismos de respaldo, la capacidad instalada y la articulación con el datacenter alterno.
- Como resultado, se obtendrá un diagnóstico del estado de las plataformas centrales, identificando brechas y acciones necesarias para su estabilización y entrada en operación.

3.5.4 Consideraciones Técnicas y Operativas:

Para asegurar la implementación efectiva y la operación continua de las soluciones de seguridad en la UNP, es fundamental tener en cuenta un conjunto de consideraciones técnicas y operativas que guiarán tanto a los especialistas como a los equipos internos. Estas consideraciones abordan aspectos clave que afectan la infraestructura, el flujo de trabajo, la integración de tecnologías y la respuesta ante incidentes.

3.5.5 Assumptions, Condiciones y Prerrequisitos:

Para que los especialistas en seguridad informática puedan comenzar a trabajar de manera efectiva y asegurar una protección integral de los activos de la UNP, es necesario cumplir con las siguientes condiciones y prerrequisitos:

3.5.6 Acceso a Credenciales de Dominio y Sistemas Críticos:

- Usuarios y contraseñas de Dominio: Se deben proporcionar a los especialistas las credenciales necesarias para acceder al dominio de la UNP, incluyendo privilegios administrativos que les permitan configurar y gestionar las soluciones de seguridad.

- Usuarios y contraseñas para Equipos y Plataformas: Se requerirá acceso a las cuentas de administrador en los dispositivos Paloalto, EDR, SIEM, WAF y Sandbox.
- Ubicación Física de los Equipos: Es fundamental que los especialistas conozcan la ubicación exacta de los equipos de seguridad dentro del datacenter principal y cualquier otro sitio relevante. Esto incluye acceso controlado a salas de servidores y áreas restringidas donde se encuentren los dispositivos.

3.5.7 Documentación Técnica y Configuraciones Actuales:

- Mapas de Red y Arquitectura de Seguridad: Se deberá proporcionar a los especialistas documentación detallada que incluya el esquema de la red, las configuraciones actuales de seguridad, y cualquier política de seguridad existente que deba ser considerada.
- Documentos de Configuración Previa: Acceso a la configuración actual de los dispositivos de seguridad (firewalls, SIEM, EDR, etc.) para que los especialistas puedan revisar y entender el estado actual antes de realizar cambios o mejoras.

3.5.8 Coordinación de Recursos y Comunicación:

Reuniones Iniciales: Programación de reuniones de inicio para alinear expectativas, revisar el alcance de los trabajos, y establecer un calendario de actividades.

Cumplir con estos prerrequisitos permitirá que los especialistas comiencen sus actividades de manera eficiente, garantizando una integración fluida con la infraestructura existente y un fortalecimiento inmediato de la seguridad en la UNP.

3.6 Activación de línea de servicios en sede - Conectividad LAN y WLAN

3.6.1 Introducción al Servicio

El servicio de conectividad LAN (Local Area Network) y WLAN (Wireless Local Area Network) es esencial para garantizar el acceso a los sistemas de información, aplicaciones, bases de datos y servicios de internet en todas las sedes de la Unidad Nacional de Protección (UNP). La activación de estos servicios asegura una conectividad eficiente y continua, respaldada por un soporte técnico robusto para todas las operaciones críticas de la entidad.

3.6.2 Estructura Operativa y Roles

Líder de Servicios en Sede: será responsable de dirigir y gestionar integralmente esta línea, garantizando la operación de la infraestructura de redes y comunicaciones (LAN, WLAN, WAN), la Línea de Emergencia Vida #103 y el NOC. Asegurará el cumplimiento de los ANS, la aplicación de ITIL v4, la coordinación con proveedores, la gestión de riesgos y la mejora continua, actuando como principal interlocutor técnico ante la Entidad.
Especialista de Redes y Comunicaciones: Es responsable de la administración y soporte de la infraestructura LAN y WLAN, asegurando su operación óptima. Cuenta con experiencia en diseño, implementación y gestión de redes, con conocimiento certificable en WAN, LAN, firewalls, enrutamiento dinámico y troubleshooting avanzado, garantizando la solución eficiente de incidentes.

3.6.3 Proceso de Activación:

69		5. Linea de Servicios en Sede	1 día	mar 30/06/2	mar 30/06/2		UT
70		Conectividad LAN y WLAN	1 día	mar 30/06/2	mar 30/06/2		UT
71		Servicio de gestión y administración de conectividad LAN/WLAN en sede	1 día	mar 30/06/26	mar 30/06/26	44	UT
72		Activación	1 día	mar 30/06/2	mar 30/06/2		UT
73		Solución integral de conectividad Línea vida 103	1 día	mar 30/06/26	mar 30/06/26		UT
74		Activacion	1 día	mar 30/06/2	mar 30/06/2		UT
75		Servicio de NOC	1 día	mar 30/06/2	mar 30/06/2		UT
76		Activacion	1 día	mar 30/06/2	mar 30/06/2		UT
77		Personal Requerido	1 día	mar 30/06/2	mar 30/06/2		UT

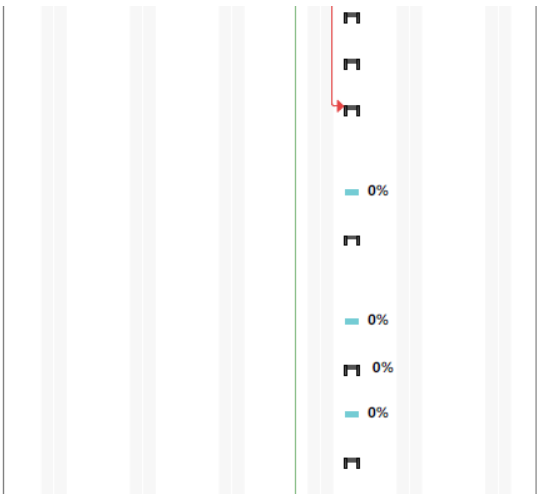


Ilustración 7 Activación Línea de Servicios en Sede

- Durante la fase de transición, se realizará la activación de los servicios en sede mediante la recepción y validación de las condiciones operativas de las diferentes sedes a nivel nacional. Este proceso incluye el levantamiento de información técnica de la infraestructura instalada, tales como redes LAN y WLAN, equipos de comunicaciones y puestos de trabajo, con el fin de establecer su estado actual y condiciones de funcionamiento.
- Posteriormente, se llevará a cabo la verificación de la infraestructura de red en cada sede, evaluando la conectividad interna, la cobertura inalámbrica y el desempeño de los dispositivos de red, así como la identificación de posibles fallas o limitaciones en el servicio.
- Se procederá con la activación del soporte en sitio, definiendo el esquema de atención presencial, articulado con la mesa de servicio y los niveles de soporte establecidos, para la gestión de incidentes y requerimientos de los usuarios.
- Adicionalmente, se validará la conectividad de las sedes hacia los servicios centrales, verificando el acceso a aplicaciones y plataformas, así como el desempeño de la comunicación con el datacenter.
- Finalmente, se ejecutarán pruebas de operación y estabilización del servicio en cada sede, permitiendo identificar brechas, necesidades de mejora y acciones correctivas, con el fin de garantizar la adecuada prestación del servicio en la fase de operación.

3.6.4 Consideraciones Técnicas y Operativas:

- **Redundancia y Alta Disponibilidad:** Todos los componentes críticos de la red deben estar configurados con redundancia para evitar interrupciones en el servicio.
- **Seguridad de la Red:** Deben existir medidas de seguridad robustas, como segmentación de la red, firewalls, y autenticación segura, para proteger la red contra amenazas externas e internas.
- **Cobertura Nacional:** Garantizar que el servicio LAN y WLAN esté disponible en todas las sedes de la UNP a nivel nacional, cumpliendo con los estándares de calidad y disponibilidad.
- **Operación Basada en ITIL:** La gestión y operación de la infraestructura LAN y WLAN deben alinearse con las prácticas ITIL v4, asegurando la eficiencia en la gestión de incidentes, problemas, cambios y niveles de servicio.

3.6.5 Assumptions, Condiciones y Prerrequisitos

- **Assumptions:** Las herramientas de gestión de red necesarias estarán completamente operativas y accesibles.
- **Condiciones:** La infraestructura física en todas las sedes debe estar habilitada para la posible instalación de equipos de red, incluyendo espacios adecuados para racks de servidores y puntos de acceso.La disponibilidad de energía regulada y respaldo (UPS) es fundamental para garantizar la continuidad del servicio en caso de fallas eléctricas.
- **Prerrequisitos:** Todos los equipos necesarios para la conectividad LAN y WLAN deben estar disponibles y preconfigurados antes de la activación.

Las herramientas de monitoreo y gestión de red deben estar configuradas y probadas para asegurar su capacidad de soportar las operaciones de la red en tiempo real.
El acceso al datacenter principal y centros cableados alternos debe ser exclusivo por parte del personal administrador de la UT, para esto se requiere que estos puntos cuenten con control de acceso.

3.6.6 Dimensionamiento del Equipo de Trabajo:

Entendemos la relevancia de contar con un equipo de trabajo debidamente dimensionado para garantizar la calidad y eficiencia en la prestación de los servicios requeridos por la Unidad Nacional de Protección (UNP). Como proveedor, nos basamos en nuestra vasta experiencia y conocimiento especializado para definir el número de profesionales necesarios para cada rol, asegurando que el proyecto se ejecute de manera óptima y cumpliendo con los estándares más altos.

De acuerdo con los términos del contrato, el dimensionamiento del personal es una prerrogativa del proveedor, y hemos realizado este proceso con la intención de maximizar el valor y la calidad del servicio ofrecido. Nuestro enfoque, aunque no requiere una justificación técnica detallada para cada posición, está alineado con las mejores prácticas de la industria (ITIL V4 y PMI), asegurando que las necesidades específicas de la UNP sean completamente satisfechas.

Nos comprometemos a asignar el equipo necesario para alcanzar los objetivos del proyecto, y estamos seguros de que nuestro dimensionamiento es adecuado para asegurar el éxito de este.

4 Gestión de Riesgos durante la Activación:

Durante la fase de inicio y transición se identificaron riesgos críticos y altos que pueden afectar la ejecución del contrato, entre ellos:

Riesgos operativos clave

- No disponibilidad de personal TIC o especializado
- Baja capacitación del recurso humano
- Falta de ambientes de pruebas y herramientas
- Retrasos en contratación de personal

Riesgos de gestión y gobernanza

- Comunicación inadecuada con el cliente

- Falta de seguimiento y control documental
- Retrasos en entrega de documentación
- Falta de aprobaciones para avanzar actividades

4.1 Estrategia de mitigación durante la transición

Para reducir el impacto de los riesgos identificados, se establecen las siguientes acciones estratégicas:

Gestión operativa

- Validación previa de recursos, accesos y herramientas
- Asignación de personal clave y recursos backup
- Verificación de ambientes de trabajo

Gestión de gobierno y comunicación

- Implementación formal del plan de comunicaciones
- Seguimiento semanal mediante comités
- Registro de decisiones en actas

Gestión documental

- Definición de cronogramas de entregables
- Validación interna de documentos antes de entrega
- Control de calidad documental

Seguridad y continuidad

- Implementación de controles de acceso
- Monitoreo de infraestructura
- Definición de plan de contingencia y respaldo

4.2 Plan de trabajo de transición

El plan se ejecuta en tres fases:

Fase 1 – Alistamiento

- Revisión contractual y técnica
- Validación de recursos (humanos y tecnológicos)
- Definición de cronograma base

Fase 2 – Ejecución de transición

- Transferencia de conocimiento
- Habilitación de accesos e infraestructura
- Validación de servicios y pruebas iniciales

Fase 3 – Estabilización

- Seguimiento a operación
- Ajustes a procesos y controles
- Monitoreo de riesgos residuales

4.3 Seguimiento y control

El monitoreo del proceso de transición se realizará mediante:

- Reuniones periódicas (mensuales)
- Informes de avance
- Control de cumplimiento del cronograma
- Evaluación de efectividad de controles

La mayoría de los controles definidos son preventivos y manuales, con soporte en cronogramas, actas y reportes operativos.

5 Estrategia de Comunicación durante la Activación:

Para garantizar la adecuada ejecución de la etapa de Activación de los Servicios, las actividades de coordinación serán lideradas de manera conjunta por el Gerente de Proyecto, el Gerente de Operaciones, los Líderes de Línea y el Líder de Proyecto PMO, quienes serán los responsables de gestionar la comunicación, el seguimiento y la articulación de las actividades con la Entidad.

A continuación, se presenta la matriz de comunicaciones, en la cual se relacionan los responsables de cada rol, incluyendo su perfil, nombre, correo electrónico y número de contacto, con el fin de facilitar los canales de comunicación y asegurar una atención oportuna durante la ejecución del proyecto.

CARGO	USUARIO	CORREO CORPORATIVO	CELULAR
Gerente Proyecto	Francisco Teran	Francisco.Teran@utserviciosssc.com	3228473931
Gerente de Operaciones	Jairo Yesid Rodriguez	Jairo.rodriguez@utserviciosssc.com	3008124444
Líder Gestión de Servicios	Carlos Ramirez	Carlos.ramirez@utserviciosssc.com	3142504571
Líder Servicios en Sede	Yedinson Dario Granada	Yedinson.granada@utserviciosssc.com	3187350414
Líder Servicios Centrales	Daniel Bernardo Zarate	Daniel.zarate@utserviciosssc.com	3124683267
Líder de Proyecto PMO	Patricia Alvarez	patricia.alvarez@utserviciosssc.com	3113618435

La comunicación efectiva constituye un factor clave para garantizar el adecuado desarrollo de la fase de transición, operabilidad y la correcta coordinación entre las partes. Para tal fin, se establecen los siguientes mecanismos de comunicación, los cuales serán utilizados de acuerdo con las necesidades del proyecto y los lineamientos definidos por la Entidad:

- Reuniones de seguimiento: Se realizarán con la periodicidad que requiera el proyecto, con el propósito de revisar el avance de las actividades, gestionar riesgos, resolver novedades, coordinar acciones y asegurar el cumplimiento de los compromisos establecidos.
- Informes periódicos: Se presentarán informes mensuales de gestión, conforme a las condiciones y periodicidad establecidas contractualmente, incluyendo el avance de las actividades, cumplimiento de entregables, indicadores, riesgos, novedades y acciones de mejora.
- Oficios y comunicaciones formales: Se emitirán cuando sea necesario para formalizar solicitudes, notificaciones, requerimientos, aprobaciones o cualquier otra comunicación relevante para la adecuada ejecución y seguimiento del proyecto, garantizando la trazabilidad de la información.

6 Responsabilidades asociadas a la gestión de activos de TI:

6.1 Metodología de Gestión de Activos de TI

La gestión de activos de TI en la UNP se llevará a cabo siguiendo las mejores prácticas de ITIL v4, utilizando la herramienta Ivanti para administrar y mantener actualizada la Base de Datos de Gestión de la Configuración (CMDB). Desde el inicio del contrato, se recibirá un inventario inicial de todos los activos tecnológicos, asegurando que la CMDB refleje fielmente todos los cambios en la infraestructura.

6.2 Consulta y Actualización de Información

Ivanti permitirá la consulta en tiempo real de la información sobre los activos, facilitando a los usuarios autorizados el acceso a detalles técnicos, históricos de mantenimiento y asignaciones. La CMDB será actualizada continuamente para reflejar cualquier intervención, reasignación o cambio en los activos.

6.3 Generación de Reportes

La herramienta Ivanti será utilizada para generar reportes basados en criterios técnicos y operativos definidos por la UNP. Esto incluirá reportes de asignación de equipos por funcionario, así como reportes de mantenimiento y fechas de expiración de garantías, lo que permitirá una gestión proactiva y planificada de los recursos tecnológicos. Esta información debe ser entregada inicialmente por la UNP con el fin de garantizar su mantenimiento.

6.4 Control de Fechas de Mantenimiento y Expiración de Garantías

Todas las fechas de mantenimiento correctivo se registran en Ivanti mediante el módulo de incidentes, garantizando que los equipos reciban el mantenimiento adecuado a tiempo. Además, se monitorearán las fechas de expiración de garantías para gestionar posibles renovaciones o reemplazos de acuerdo con las políticas de la UNP.

6.5 Administración de la CMDB

La CMDB será mantenida completa y precisa, alineada con los estándares de ITIL v4. Se realizarán auditorías regulares para verificar la exactitud de la información, asegurando que todos los activos de TI estén correctamente documentados y gestionados.

6.6 Responsabilidades del Contratista

La UT es responsable de la documentación y reporte continuo de los activos de TI, garantizando el cumplimiento de las prácticas de ITIL v4 y la actualización constante de la CMDB en Ivanti. Además, deberá asegurar que su equipo esté capacitado en el uso de la herramienta y en las prácticas de gestión establecidas.

Esta metodología proporciona un control riguroso y eficiente sobre los activos de TI de la UNP, asegurando que los recursos estén siempre disponibles y en óptimas condiciones operativas.

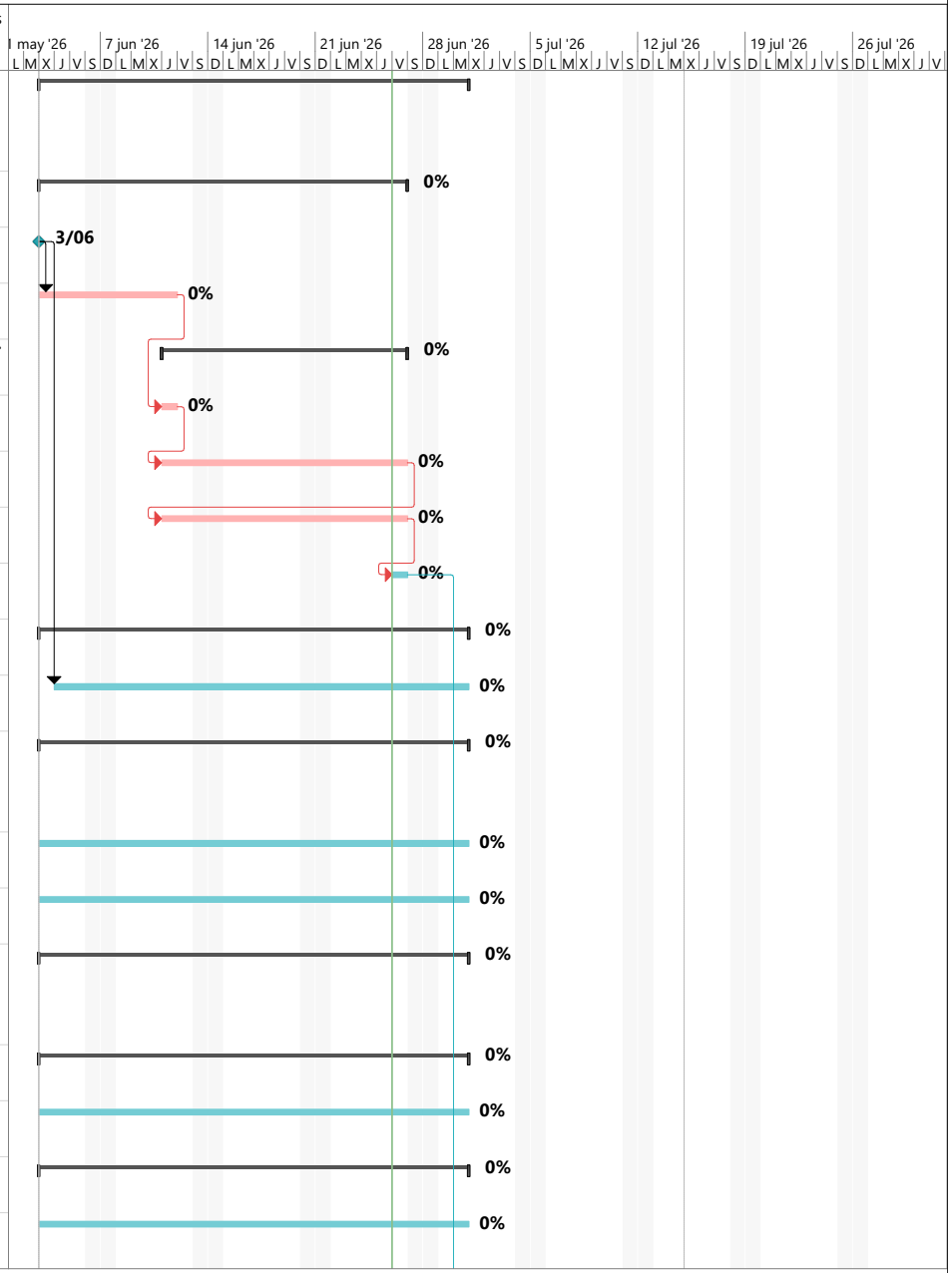
7 Anexos

- Cronograma de activación de servicios.
- Matriz de Riesgos
- Plan de comunicaciones

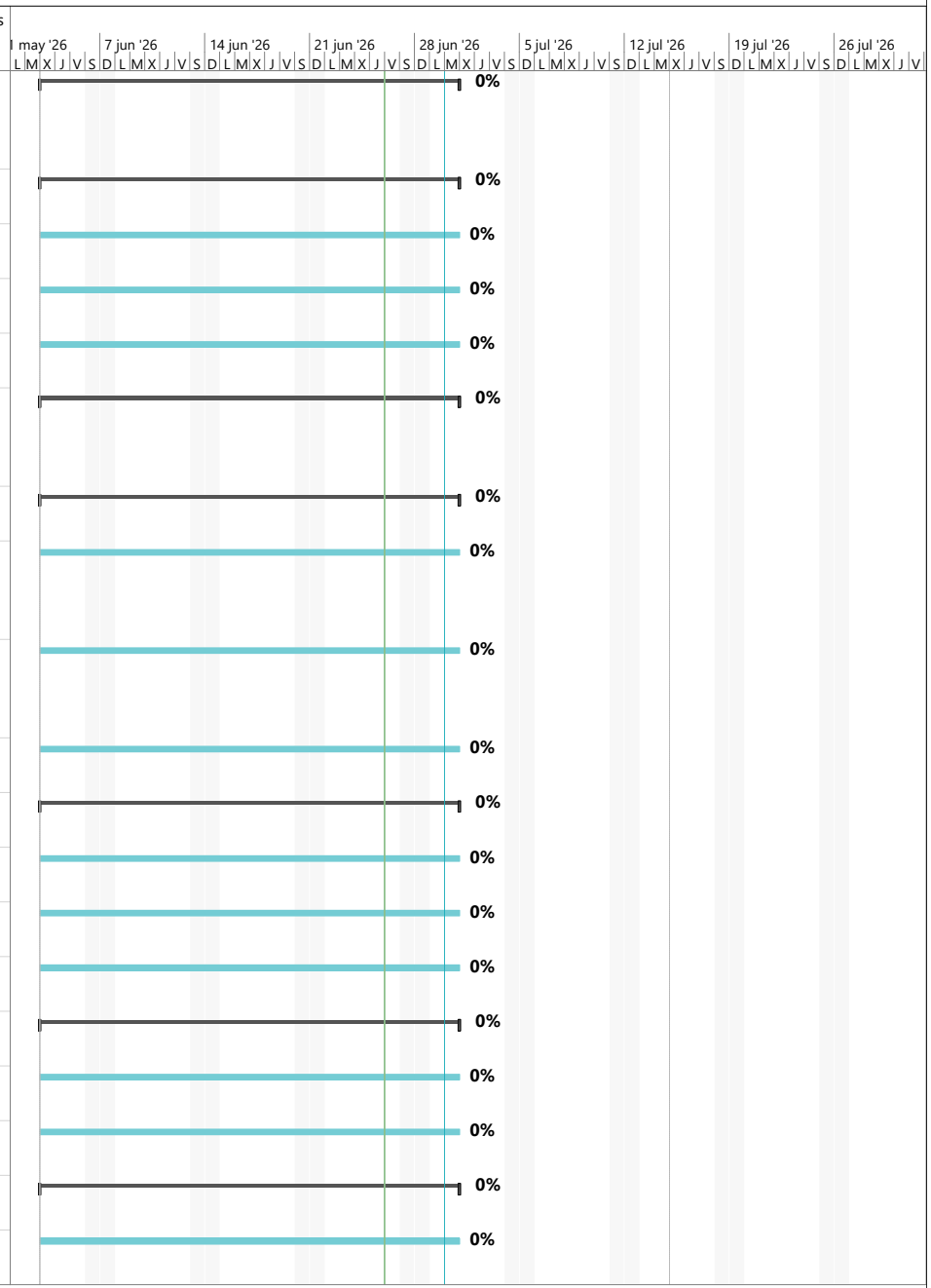
8 Cuadro de aprobación.

Elaboró	Revisó	Aprobó
Patricia Alvarez Vega **Líder de Proyecto PMO**	Jairo Yesid Rodriguez **Gerente de Operaciones**	Francisco José Terán **Gerente de Proyecto**
Fecha: 30-junio-2026	Fecha: 30-junio-2026	Fecha: 01-julio-2026

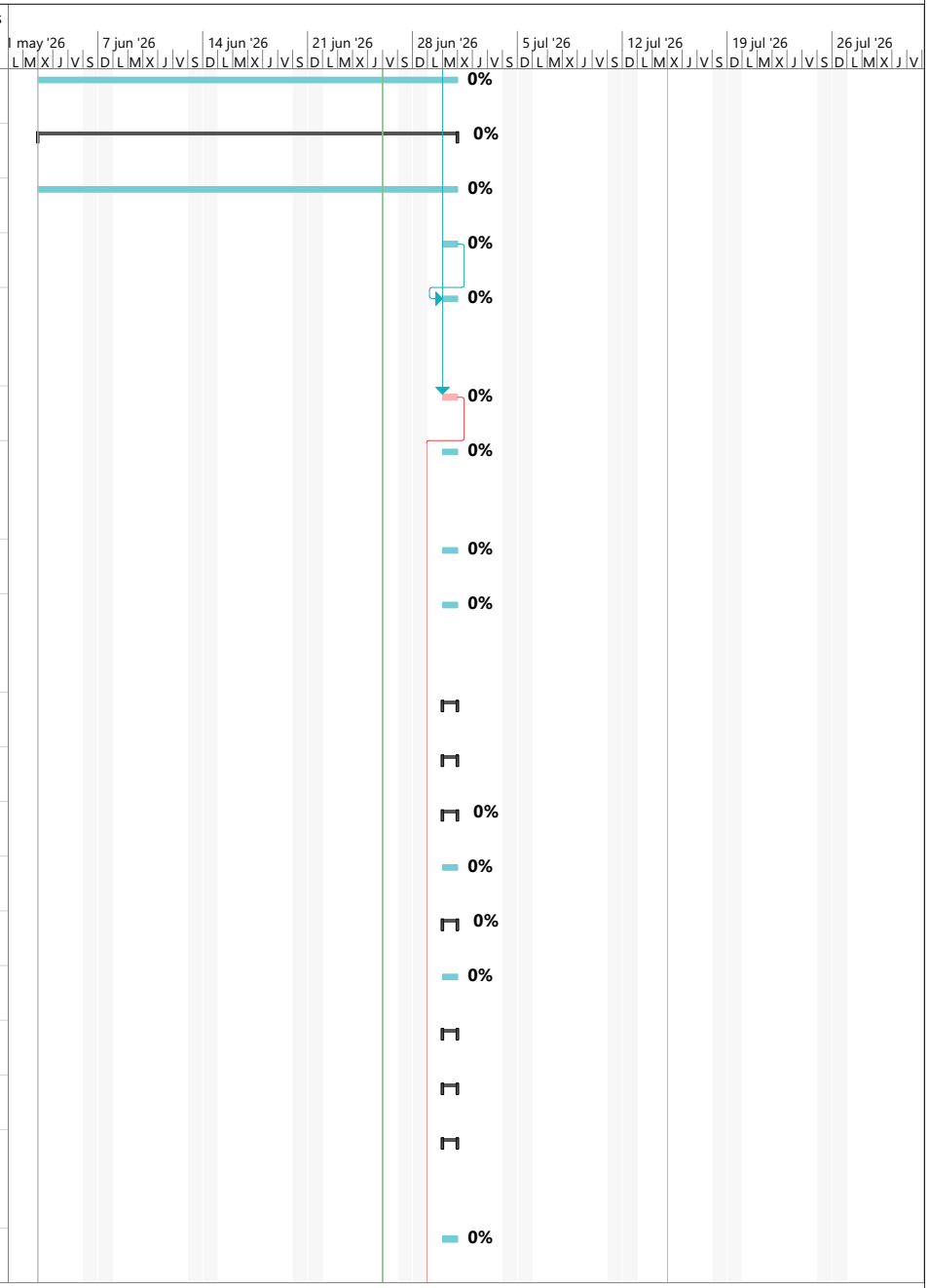
Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predec	Nombres de los recursos
1		**CRONOGRAMA DE ACTIVACIÓN DE SERVICIOS - CTO 2546-2O26**	**20 días**	**mié 3/06/26**	**mar 30/06/26**		**UT**
2		**1. INICIO**	**18 días**	**mié 3/06/26**	**vie 26/06/26**		**UNP**
3		Adjudicacion Contrato	0 días	mié 3/06/26	mié 3/06/26		UNP
4		Perfeccionamiento y Firma contrato	7 días	mié 3/06/26	jue 11/06/26	3	UNP
5		**Polizas Contrato**	**12 días**	**jue 11/06/26**	**vie 26/06/26**		**UNP;UT**
6		Envio polizas para aprobación UNP	1 día	jue 11/06/26	jue 11/06/26	4	UT
7		Revisión Polizas UNP	12 días	jue 11/06/26	vie 26/06/26	6	UNP
8		Ajuste polizas	12 días	jue 11/06/26	vie 26/06/26	7	UT
9		Polizas aprobadas SECOP	1 día	vie 26/06/26	vie 26/06/26	8	UNP
10		**2. PLANEACIÓN**	**20 días**	**mié 3/06/26**	**mar 30/06/2**		**UT**
11		Planeacion activación servicios	19 días	jue 4/06/26	mar 30/06/2	3	UT
12		**Planeación activación Línea Gestion de Servicios**	**20 días**	**mié 3/06/26**	**mar 30/06/26**		**UT**
13		Mesa de ayuda y Soporte en Sitio	20 días	mié 3/06/26	mar 30/06/2		UT
14		Soporte remoto y en Sitio (LV103)	20 días	mié 3/06/26	mar 30/06/2		UT
15		**Planeacion activaciòn Línea de Servicios Centrales**	**20 días**	**mié 3/06/26**	**mar 30/06/26**		**UT**
16		**Datacenter Principal**	**20 días**	**mié 3/06/26**	**mar 30/06/2**		**UT**
17		Datacenter Principal	20 días	mié 3/06/26	mar 30/06/2		UT
18		**Datacenter Alterno**	**20 días**	**mié 3/06/26**	**mar 30/06/2**		**UT**
19		Datacenter alterno	20 días	mié 3/06/26	mar 30/06/2		UT



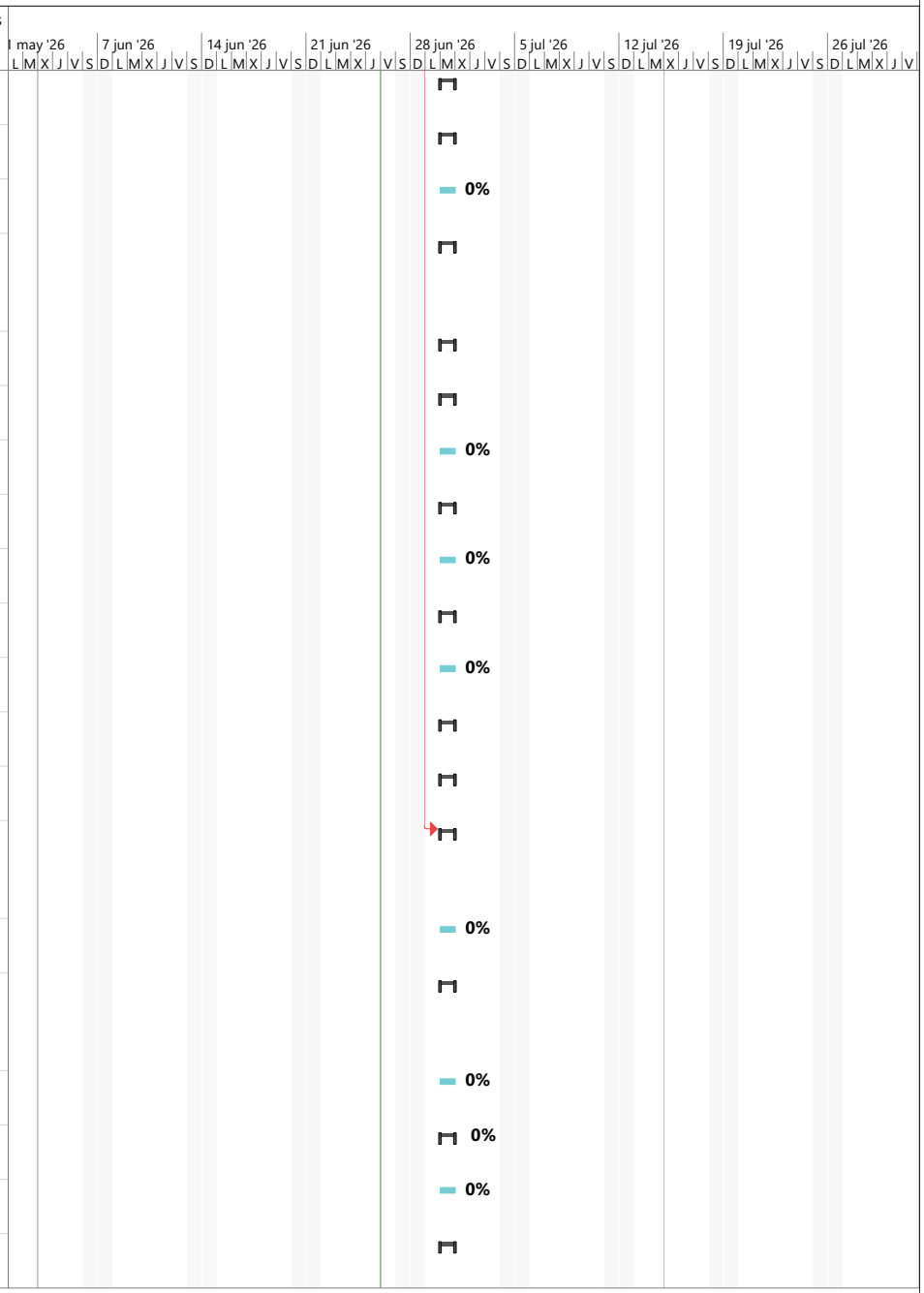
Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predec	Nombres de los recursos
20		**Planeacion Activacion Soporte Especializado Plataformas Centrales**	**20 días**	**mié 3/06/26**	**mar 30/06/26**		**UT**
21		**Seguridad de la información**	**20 días**	**mié 3/06/26**	**mar 30/06/2**		**UT**
22		Licenciamiento Plataformas de segur	20 días	mié 3/06/26	mar 30/06/2(		UT
23		Servicios de Seguridad CSOC	20 días	mié 3/06/26	mar 30/06/2(		UT
24		Admin Plataformas de Seguridad	20 días	mié 3/06/26	mar 30/06/2(		UT
25		**Planeacion Activación Linea de Servicios en Sede**	**20 días**	**mié 3/06/26**	**mar 30/06/26**		**UT**
26		**Conectividad LAN y WLAN**	**20 días**	**mié 3/06/26**	**mar 30/06/2**		**UT**
27		Servicio de gestión y administración de conectividad LAN/WLAN en sede	20 días	mié 3/06/26	mar 30/06/26		UT
28		Solución integral de conectividad Línea vida 103	20 días	mié 3/06/26	mar 30/06/26		UT
29		Servicio de NOC	20 días	mié 3/06/26	mar 30/06/2(		UT
30		**Planeación Activacion Personal**	**20 días**	**mié 3/06/26**	**mar 30/06/2**		**UT**
31		Busqueda, selección y contratación per	20 días	mié 3/06/26	mar 30/06/2(		UT
32		Hojas de vida personal requeridos	20 días	mié 3/06/26	mar 30/06/2(		UT
33		Matriz de Hojas de Vida	20 días	mié 3/06/26	mar 30/06/2(		UT
34		**Hojas de vida personal Adicional**	**20 días**	**mié 3/06/26**	**mar 30/06/2**		**UT**
35		Especialistas	20 días	mié 3/06/26	mar 30/06/2(		UT
36		Tecnicos adiciones de soporte	20 días	mié 3/06/26	mar 30/06/2(		UT
37		**Planeacion condiciones activación Servic**	**20 días**	**mié 3/06/26**	**mar 30/06/2**		**UT**
38		Revisión alcance servicios	20 días	mié 3/06/26	mar 30/06/2(		UT



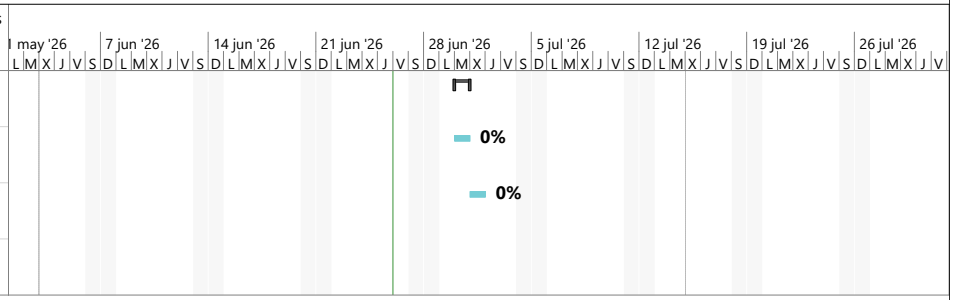
Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predec	Nombres de los recursos
39		Transición y ANSs	20 días	mié 3/06/26	mar 30/06/26		UT
40		**3. EJECUCIÓN**	**20 días**	**mié 3/06/26**	**mar 30/06/26**		**UNP**
41		Preparación documentación para Acta Ini	20 días	mié 3/06/26	mar 30/06/26		UT
42		Reunión Entendimiento	1 día	mar 30/06/26	mar 30/06/26		UNP;UT
43		Entrega documentación a UNP para Acta de Inicio	1 día	mar 30/06/26	mar 30/06/26	42	UT
44		Reunión Acta de inicio	1 día	mar 30/06/26	mar 30/06/26	9	UNP;UT
45		Revisión condiciones de UT para Activacion Servicios - Plan de trabajo	1 día	mar 30/06/26	mar 30/06/26		UNP;UT
46		Firma Acta de Inicio	1 día	mar 30/06/26	mar 30/06/26		UNP;UT
47		Aprobación UNP condiciones Activación Servicios	1 día	mar 30/06/26	mar 30/06/26		UNP
48		**Activación Servicios**	**1 día**	**mar 30/06/26**	**mar 30/06/26**		**UT**
49		**1. Línea de gestión de servicios**	**1 día**	**mar 30/06/26**	**mar 30/06/26**		**UT**
50		**1.1 Mesa de ayuda y Soporte en Siti**	**1 día**	**mar 30/06/26**	**mar 30/06/26**		**UT**
51		Activación	1 día	mar 30/06/26	mar 30/06/26		UT
52		**1.2 Soporte Remoto y en Sitio (LV10**	**1 día**	**mar 30/06/26**	**mar 30/06/26**		**UT**
53		Activación	1 día	mar 30/06/26	mar 30/06/26		UT
54		**2. Línea de Servicios Centrales**	**1 día**	**mar 30/06/26**	**mar 30/06/26**		**UT**
55		**Datacenter Principal**	**1 día**	**mar 30/06/26**	**mar 30/06/26**		**UT**
56		**2.1.1 a 2.1.6 Colocación en Datacenter Principal**	**1 día**	**mar 30/06/26**	**mar 30/06/26**		**UT**
57		Activacion	1 día	mar 30/06/26	mar 30/06/26		UT

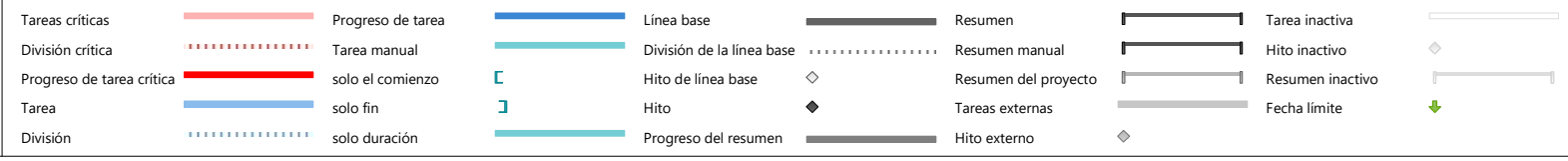


Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predec	Nombres de los recursos
58		**3. Datacenter Alterno**	**1 día**	**mar 30/06/2**	**mar 30/06/2**		**UT**
59		**3.1 a 3.6 Datacenter alterno**	**1 día**	**mar 30/06/2**	**mar 30/06/2**		**UT**
60		Activación	1 día	mar 30/06/2(	mar 30/06/2(		UT
61		**4. Soporte Especializado Plataformas Centrales**	**1 día**	**mar 30/06/26**	**mar 30/06/26**		**UT**
62		**4.1 Seguridad de la información**	**1 día**	**mar 30/06/2**	**mar 30/06/2**		**UT**
63		**Licenciamiento Plataforma de Seg**	**1 día**	**mar 30/06/2**	**mar 30/06/2**		**UT**
64		Activación	1 día	mar 30/06/2(	mar 30/06/2(		UT
65		**Servicios de Seguridad CSOC**	**1 día**	**mar 30/06/2**	**mar 30/06/2**		**UT**
66		Activación	1 día	mar 30/06/2(	mar 30/06/2(		UT
67		**Admin Plataformas de Seguridad**	**1 día**	**mar 30/06/2**	**mar 30/06/2**		**UT**
68		Activación	1 día	mar 30/06/2(	mar 30/06/2(		UT
69		**5. Linea de Servicios en Sede**	**1 día**	**mar 30/06/2**	**mar 30/06/2**		**UT**
70		**Conectividad LAN y WLAN**	**1 día**	**mar 30/06/2**	**mar 30/06/2**		**UT**
71		**Servicio de gestión y administración de conectividad LAN/WLAN en sede**	**1 día**	**mar 30/06/26**	**mar 30/06/26**	**44**	**UT**
72		Activación	1 día	mar 30/06/2(	mar 30/06/2(		UT
73		**Solución integral de conectividad Línea vida 103**	**1 día**	**mar 30/06/26**	**mar 30/06/26**		**UT**
74		Activacion	1 día	mar 30/06/2(	mar 30/06/2(		UT
75		**Servicio de NOC**	**1 día**	**mar 30/06/2**	**mar 30/06/2**		**UT**
76		Activacion	1 día	mar 30/06/2(	mar 30/06/2(		UT
77		**Personal Requerido**	**1 día**	**mar 30/06/2**	**mar 30/06/2**		**UT**



Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predec	Nombres de los recursos
78		**Personal en sitio**	**1 día**	**mar 30/06/2**	**mar 30/06/2**		**UT**
79		Activaciòn	1 día	mar 30/06/2	mar 30/06/2		UT
80		**INICIO CRONOGRAMA GENERAL DEL PROYEC**	1 día	mié 1/07/26	mié 1/07/26		UNP;UT
81							




Tareas críticas
División crítica
Progreso de tarea crítica
Tarea
División
Progreso de tarea
Tarea manual
solo el comienzo
solo fin
solo duración
Línea base
División de la línea base
Hito de línea base
Hito
Progreso del resumen
Resumen
Resumen manual
Resumen del proyecto
Tareas externas
Hito externo
Tarea inactiva
Hito inactivo
Resumen inactivo
Fecha límite