| | |
|---|---|
| **Nombre Comercial del Bien o Servicio** | **PERFILES PROFESIONALES — Personal mínimo requerido del PROVEEDOR para la prestación de los cinco (5) dominios contratados y de los servicios transversales de infraestructura y centro de datos que los soportan.** |
| **Calidad** | El Contratista debe garantizar que el personal asignado cumpla las normas, certificaciones y experiencia requeridas. Las certificaciones deben estar vigentes durante la ejecución del contrato. El servicio debe prestarse aplicando mejores prácticas y marcos de referencia reconocidos: ITIL v4, ISO/IEC 27001, ISO/IEC 27002, ISO 20000, ISO 22301, COBIT 2019, NIST CSF, OWASP, Ley 1581 de 2012 y normativa asociada de protección de datos personales, Modelo de Seguridad y Privacidad de la Información (MSPI) del Estado colombiano, Circular Externa No. 008 de 2017 de la SIC, Resolución 1126 de 2021 del MinTIC. |
| **Generalidades** | El presente anexo describe los perfiles profesionales mínimos exigibles al PROVEEDOR para la prestación de los servicios contratados en los cinco (5) dominios del proceso: Conectividad, Seguridad, Servicios, Videoconferencia y Cableado, así como los perfiles transversales de infraestructura y centro de datos (P7) que soportan la operación de dichos dominios. Es la fuente única de verdad para la definición de los perfiles del PROVEEDOR —formación, experiencia, certificaciones, responsabilidades y disponibilidad—; las cantidades mínimas y dedicaciones son las incorporadas en cada ficha, coincidentes con la pestaña «P6. Perfiles» del Formato de Oferta Económica. En caso de discrepancia entre el presente anexo y la pestaña «P6. Perfiles» del Formato 8 – Oferta Económica, prevalecerá lo establecido en el presente Anexo Técnico 6 respecto de las cantidades, perfiles y dedicaciones exigidos; el Formato 8 deberá diligenciarse en concordancia con este anexo. Los demás anexos del proceso (Anexo 1 — Conectividad, Anexo 2 — Seguridad, Anexo 3 — Videoconferencia, Anexo 4 — Cableado, Anexo 7 — Protocolo de Transición) remiten al presente anexo para el detalle de los perfiles.<br><br>Clasificación de perfiles:<br><br>• **Roles estratégicos transversales (P1)**<br>• **Perfiles técnicos de Conectividad (P2)**<br>• **Perfiles técnicos de Seguridad (P3)**<br>• **Perfiles técnicos de Servicios Mesa de Ayuda y Observabilidad (P4)**<br>• **Perfiles técnicos de Videoconferencia (P5)**<br>• **Perfiles técnicos de Cableado (P6)**<br>• **Perfiles de Infraestructura (P7)**<br><br>Los entregables mensuales por perfil se describen en el numeral P8 y las reglas generales aplicables a todo el personal en el numeral P9. |
| **Requisitos generales** | Para todos los perfiles técnicos se establecen obligaciones operativas mínimas orientadas a garantizar la trazabilidad, la calidad del servicio y el cumplimiento normativo. Cada integrante debe registrar y gestionar incidentes, requerimientos y cambios dentro de la herramienta ITSM institucional, asegurando un seguimiento completo y verificable. Asimismo, es indispensable cumplir y evidenciar los ANS y KPI definidos para el servicio a su cargo, incluyendo tiempos de atención, escalamiento y cierre. La documentación técnica —configuraciones, topologías, inventarios y procedimientos operativos— debe |

| | |
|---|---|
| | mantenerse actualizada y disponible, de modo que respalde la operación y facilite auditorías o procesos de continuidad.<br><br>En el marco de la operación, se espera que los técnicos ejecuten las ventanas de mantenimiento y los cambios aprobados por el comité de control de cambios, cuando estos apliquen. También deben garantizar la integridad, estructuración y legibilidad de los logs bajo su responsabilidad, asegurando su disponibilidad para procesos de auditoría o investigación. La coordinación de escalamiento con los fabricantes debe realizarse de manera oportuna, conservando evidencias de casos, diagnósticos y acciones adelantadas. A ello se suma la verificación proactiva del estado de los servicios y la ejecución de acciones preventivas que mitiguen riesgos operativos. La gestión y protección de credenciales y accesos debe observar estrictamente el principio de mínimo privilegio y los controles definidos por la FGN. Todas las actividades deben alinearse con la normativa vigente, incluyendo la Ley 1581 de 2012, el MSPI y las políticas internas. Finalmente, cada responsable debe entregar reportes y evidencias mensuales sobre el estado, capacidad, riesgos y oportunidades de mejora del componente que opera.<br><br>En cuanto a los roles estratégicos, sus obligaciones se orientan al gobierno integral del servicio y a la articulación entre los distintos dominios tecnológicos. Les corresponde dirigir el cumplimiento de la Ley 1581, el MSPI y las políticas institucionales, así como definir, controlar y evaluar los ANS y KPI, impulsando planes de mejora continua con seguimiento mensual. Deben asegurar la integración operativa entre conectividad, seguridad, SOC/NOC, ITSM y observabilidad, promoviendo una visión unificada del servicio. También es su responsabilidad aprobar y dirigir los planes de cambios mayores, gestionar el riesgo operativo y liderar la atención de incidentes mayores, incluyendo la coordinación de mesas de crisis cuando sea necesario.<br><br>Estos roles deben exigir y validar la calidad de los logs, garantizando que sean íntegros, estructurados y auditables. Asimismo, deben gobernar la relación con los fabricantes, gestionando escalamientos críticos, análisis de causa raíz y la alineación con los roadmaps tecnológicos. Les corresponde asegurar la capacidad, disponibilidad y continuidad de los servicios, incluyendo esquemas de alta disponibilidad y recuperación ante desastres cuando aplique. La calidad documental y la trazabilidad contractual —actas, reportes y evidencias— también forman parte de sus responsabilidades, junto con la presentación de informes ejecutivos mensuales y recomendaciones accionables al Supervisor y a la FGN.<br><br>Los requisitos específicos por perfil (P1 a P7), los entregables mensuales (P8) y las reglas generales (P9) se desarrollan en detalle en la sección de Requisitos Específicos, donde se precisan las responsabilidades diferenciadas según el rol. |
| **Requisitos específicos** | |
| **P1. Roles estratégicos transversales** | **P1.1. Gerente de Proyecto Presencial**<br>• Objeto y rol: Dirección y control integral del proyecto. Único punto de contacto del PROVEEDOR ante la FGN.<br>• Cantidad mínima: uno (1). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Título profesional en Ingeniería de |

| | | |
|---|---|---|
| | | Sistemas, Telecomunicaciones, Electrónica o afines.<br>• Experiencia: Mínima de diez (10) años de experiencia profesional y dos (2) años de experiencia específica en Gerencia de Proyectos TIC, con experiencia comprobable en proyectos de igual o mayor complejidad al presente contrato.<br>• Certificaciones: Certificación vigente PMP del PMI o equivalente; especialización o maestría en Gerencia de Proyectos, Gestión de Proyectos o áreas afines relacionadas con la gerencia, dirección o gestión de proyectos tecnológicos, gestión de servicios de tecnología, gerencia informática o transformación digital, cuya pertinencia académica se validará frente a las funciones del cargo y el alcance del proyecto; ITIL v4 o superior.<br>• Responsabilidades: Coordinar, planear y realizar seguimiento integral al contrato; liderar y supervisar el equipo humano del PROVEEDOR; servir como único punto de contacto ante la FGN; coordinar el proceso de transición; asistir a comités y reuniones de seguimiento; consolidar y presentar informes mensuales; tomar decisiones reactivas y preventivas; garantizar cumplimiento de objetivos, cronograma, ANS y obligaciones contractuales.<br>• Disponibilidad: 5×8 presencial de lunes a viernes durante toda la ejecución del contrato, con disponibilidad adicional cuando la operación lo requiera.<br>• Personal de planta: Sí, personal de planta del PROVEEDOR durante toda la ejecución. |
| | **P1.2.** | **Director Técnico**<br>• Objeto y rol: Dirección técnica transversal de todos los servicios contratados.<br>• Cantidad mínima: uno (1). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Profesional en Ingeniería de Sistemas/Telecomunicaciones/Electrónica.<br>• Experiencia: Mínima de ocho (8) años en dirección técnica de servicios TIC de gran escala.<br>• Certificaciones: ITIL v4 Strategic Leader o ITIL Strategic Leader (Version 5); mínimo una (1) certificación vigente de nivel arquitectura de un fabricante de la solución ofertada en los dominios de Conectividad o Seguridad.<br>• Responsabilidades: Aprobar diseños técnicos; validar arquitecturas; resolver escalamientos técnicos; presidir comités técnicos; garantizar |

| | |
|---|---|
| | coherencia arquitectónica entre los cinco dominios contratados.<br>• Disponibilidad: 5×8 presencial de lunes a viernes durante toda la ejecución del contrato, con disponibilidad adicional cuando la operación lo requiera. con disponibilidad ampliada para incidentes críticos.<br>• Personal de planta: Sí.<br><br>**P1.3. Jefe de Servicios**<br>• Objeto y rol: Dirección y aseguramiento de la operación del servicio.<br>• Cantidad mínima: uno (1). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Ingeniería Electrónica o afines; Especialización y/o maestría en Gerencia o Dirección de Proyectos.<br>• Experiencia: Mínima de doce (12) años de experiencia profesional y cuatro (4) años de experiencia específica en liderazgo de operaciones y proyectos de servicios de TI.<br>• Certificaciones: ITIL v4 o superior; Scrum Master / Product Owner; formación en PMI.<br>• Responsabilidades: Liderar y garantizar la correcta operación de los servicios; asegurar continuidad, calidad y mejora continua; supervisar la Mesa de Ayuda y soporte en sitio; garantizar cumplimiento de los ANS; liderar escalamientos técnicos y contractuales; validar métricas, penalizaciones y exclusiones; velar por la calidad percibida; liderar iniciativas de mejora continua; coordinar con áreas de seguridad y cumplimiento; presentar informes ejecutivos.<br>• Disponibilidad: 5×8 presencial de lunes a viernes durante toda la ejecución del contrato, con disponibilidad adicional durante incidentes críticos, ventanas de mantenimiento o eventos de alto impacto.<br>• Personal de planta: Sí.<br><br>**P1.4. Gerente de Seguridad**<br>• Objeto y rol: Dirección y gobierno del servicio gestionado de seguridad digital y ciberseguridad.<br>• Cantidad mínima: uno (1). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Profesional en Ingeniería de Sistemas/Telecomunicaciones o afines; posgrado en seguridad de la información.<br>• Experiencia: Mínima de ocho (8) años de experiencia profesional y cuatro (4) años de experiencia específica en operación de SOC y |

| | |
|---|---|
| | gestión de servicios de seguridad.<br>• Certificaciones: CEH y LCSPC o CISSP, CISM, CISA o equivalente; ISO/IEC 27001:2022 Lead Auditor y ISO/IEC 22301:2019 Lead Auditor.<br>• Responsabilidades: Dirigir el gobierno del servicio de seguridad; presidir reuniones con la FGN para revisión de postura; aprobar políticas, casos de uso, runbooks; representar al PROVEEDOR ante incidentes mayores.<br>• Disponibilidad: 5×8 presencial de lunes a viernes durante toda la ejecución del contrato, con disponibilidad 7×24 para incidentes críticos.<br>• Personal de planta: Sí.<br><br>**P1.5. Coordinador SOC**<br>• Objeto y rol: Coordinación operativa del Centro de Operaciones de Seguridad 24×7. El rol podrá estar soportado por un equipo especializado, siempre que exista un Coordinador SOC responsable ante la Entidad y se garantice la operación 24×7 del SOC.<br>• Cantidad mínima: uno (1). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Profesional en Ingeniería de Sistemas/Telecomunicaciones.<br>• Experiencia: Mínima de cinco (5) años de experiencia profesional y tres (3) años de experiencia específica en operación de SOC; experiencia en SIEM/SOAR/NDR.<br>• Certificaciones: Al menos dos (2) certificaciones vigentes en gestión y respuesta de incidentes de seguridad de la información, tales como GCIH, CHFI, CEH, ISO/IEC 27001:2022 Lead Auditor o ISO/IEC 22301:2019 Lead Auditor, o certificaciones equivalentes o funcionalmente comparables, acreditables mediante experiencia verificable y pertinencia técnica frente al rol; y certificación vigente del fabricante del SIEM efectivamente ofertado, o equivalente.<br>• Responsabilidades: Coordinar turnos del SOC 24×7; supervisar la calidad de los casos atendidos; afinar reglas de correlación; gestionar el ciclo de vida de casos de uso; liderar el equipo de analistas N1/N2.<br>• Disponibilidad: 5×8 + guardia 24×7 presencial.<br>• Personal de planta: Sí.<br><br>**P1.6. Coordinador de Agentes**<br>• Objeto y rol: Coordinación del frente de atención de Mesa de Ayuda y soporte en sitio.<br>• Cantidad mínima: uno (1). Dedicación: 100 %. |

| | |
|---|---|
| | Periodo: treinta y seis (36) meses.<br>• Estudios: Tecnólogo o profesional en Sistemas/Telecomunicaciones o afines.<br>• Experiencia: Mínima de cinco (5) años en operación ITSM/mesa de servicios; dos (2) años coordinando equipos.<br>• Certificaciones: ITIL Foundation; certificación en alguna herramienta ITSM.<br>• Responsabilidades: Gestionar productividad de la mesa; asegurar cumplimiento de ANS de atención; coordinar turnos; gestionar calidad de tickets; escalamientos a niveles superiores; capacitación continua del equipo.<br>• Disponibilidad: 5×8 presencial de lunes a viernes durante toda la ejecución del contrato, con disponibilidad adicional cuando la operación lo requiera.<br>• Personal de planta: Sí. |
| **P2. Perfiles técnicos de Conectividad** | **P2.1. Ingenieros Residentes**<br>• Objeto y rol: Operación técnica y soporte especializado del servicio en sitio.<br>• Cantidad mínima: tres (3) —dos (2) en Bogotá y uno (1) en Cali—. Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Ingeniero de Sistemas, Telecomunicaciones, Comunicaciones o afines.<br>• Experiencia: Mínima de cinco (5) años de experiencia profesional y tres (3) años de experiencia específica en proyectos de comunicaciones; posgrado en redes de datos o telecomunicaciones.<br>• Certificaciones: Certificaciones vigentes del fabricante de los equipos suministrados.<br>• Responsabilidades: Administrar y operar plataformas; gestionar incidentes y requerimientos de comunicaciones/seguridad/videoconferencia; respaldo y verificación de configuraciones; apoyo al monitoreo de la plataforma de gestión centralizada; diagnóstico y solución de fallas; planeación de capacidad; informes técnicos mensuales; visitas técnicas a sedes.<br>• Disponibilidad: Bogotá: dos (2) ingenieros residentes 5×12 (turnos de 8 h de lunes a viernes y sábados 1×6). Cali: un (1) ingeniero residente 5×8 de manera presencial.<br>• Personal de planta: Sí. |

**P2.2. Especialista en Conectividad**

• Objeto y rol: Operación de redes WAN/SD-WAN multisedes, ruteo, QoS, segmentación.
• Cantidad mínima: dos (2). Dedicación: 100 %. Periodo: treinta y seis (36) meses.
• Estudios: Profesional en Telecomunicaciones/Sistemas/Electrónica o Ingeniería en Control.
• Experiencia: Mínima de tres (3) años en redes WAN/SD-WAN multisedes; dos (2) años en gestión de cambios con ventanas y rollback.
• Certificaciones: CCNP/JNCIP o equivalente; certificación SD-WAN del fabricante ofertado.
• Responsabilidades: Operación de la red WAN/SD-WAN; afinamiento de políticas; gestión de incidentes; coordinación con carriers/ISP; mantenimiento de documentación de red.
• Disponibilidad: 5×8 presencial de lunes a viernes durante toda la ejecución del contrato con disponibilidad adicional en cortes mayores.
• Personal de planta: Sí.

**P2.3. Especialista en SDWAN**

• Objeto y rol: Operación específica de la plataforma SD-WAN nacional: orquestador, políticas, túneles dinámicos sede a sede, QoS.
• Cantidad mínima: uno (1). Dedicación: 100 %. Periodo: treinta y seis (36) meses.
• Estudios: Profesional en Telecomunicaciones/Sistemas/Electrónica.
• Experiencia: Mínima de cinco (5) años en SD-WAN empresarial; tres (3) años en la plataforma SD-WAN específica del fabricante ofertado.
• Certificaciones: Certificación SD-WAN avanzada del fabricante de la solución efectivamente ofertada, o equivalente; complemento en seguridad del mismo fabricante o certificación equivalente que acredite las mismas competencias.
• Responsabilidades: Operación del orquestador SD-WAN; políticas de selección dinámica de rutas; configuración de túneles dinámicos sede a sede; integración con SASE/SSE; QoS por aplicación; conmutación activo-activo Bogotá-Cali; integración a la plataforma de Observabilidad institucional.
• Disponibilidad: 5×8 presencial con guardia 24×7 para incidentes P1 que afecten la SD-WAN.
• Personal de planta: Sí.

**P2.4. Gestor de Transición**

| | |
|---|---|
| | • Objeto y rol: Punto único de contacto del PROVEEDOR ENTRANTE durante la fase de transición. Lidera la migración desde el PROVEEDOR SALIENTE conforme al Anexo 7.<br>• Cantidad mínima: uno (1). Dedicación: 100 %. Periodo: meses uno (1) a diez (10) del contrato.<br>• Estudios: Profesional en Ingeniería de Sistemas/Telecomunicaciones; especialización en Gerencia de Proyectos.<br>• Experiencia: Mínima de cinco (5) años de experiencia profesional y dos (2) años de experiencia específica en transiciones de servicios TIC de gran escala; experiencia comprobable en mínimo un (1) proceso similar al presente.<br>• Certificaciones: PMP o IPMA vigente; ITIL Specialist con énfasis en Plan, Implement and Control; recomendable PMI-ACP o formación adicional en gestión del cambio.<br>• Responsabilidades: Liderar el protocolo de transición (Anexo 7); presentar el Plan Detallado de Transición; coordinar cronograma de cortes por sede; gestionar el ciclo de PAT y rollback; reportar semanalmente los KPIs de transición (numeral T4 del Anexo 7); coordinar con el PROVEEDOR SALIENTE; resolver escalamientos N1; suscribir actas de activación.<br>• Disponibilidad: 7×24 durante ventanas de corte; 5×8 fuera de ventanas. Vigencia: desde D-15 hasta la firma del Acta de Cierre de Transición. Conforme a la pestaña «P6. Perfiles» del Formato de Oferta Económica, el perfil se cotiza para los meses uno (1) a diez (10) del contrato, con dedicación del cien por ciento (100 %).<br>• Personal de planta: Sí.<br><br>**P2.5. Coordinador de Salida**<br>• Objeto y rol: Punto único de contacto del PROVEEDOR SALIENTE durante la fase de transición. Garantiza la continuidad del servicio en las sedes aún no migradas, entrega la documentación e información de la operación vigente y apoya la migración conforme al Anexo 7. Este perfil corresponde al PROVEEDOR SALIENTE y, por tanto, no se cotiza en el Formato de Oferta Económica del presente proceso.<br>• Cantidad mínima: uno (1), a cargo del PROVEEDOR SALIENTE. Este perfil no se cotiza en el Formato de Oferta Económica del presente proceso.<br>• Estudios: Profesional en Ingeniería de |

| | | |
|---|---|---|
| | | Sistemas, Telecomunicaciones, Electrónica o afines.<br>• Experiencia: Mínima de cinco (5) años de experiencia profesional y dos (2) años de experiencia específica en operación o entrega de servicios TIC de gran escala.<br>• Certificaciones: ITIL v4 o equivalente; deseable formación acreditada en gerencia de proyectos.<br>• Responsabilidades: Entregar el inventario y la CMDB inicial del servicio; liderar la transferencia de conocimiento y la retirada conforme al numeral T8 del Anexo 7; mantener la operación de las sedes aún no migradas hasta su activación; notificar al PROVEEDOR ENTRANTE los cambios de infraestructura con setenta y dos (72) horas de anticipación (T3.5); apoyar las ventanas de corte y los eventos de rollback; gestionar la revocación de accesos dentro del plazo definido en T8.3; suscribir las actas de activación y el Acta de Cierre del Protocolo.<br>• Disponibilidad: Días hábiles, con guardia durante las ventanas de corte y los eventos de rollback.<br>• Personal de planta: Sí, del PROVEEDOR SALIENTE. |
| | **P2.6.** | **Operadores NOC**<br>• Objeto y rol: Monitoreo continuo del estado de la red y respuesta inicial a alarmas.<br>• Cantidad mínima: cuatro (4), en turnos rotativos para la cobertura 7×24. Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Tecnólogo en Sistemas/Telecomunicaciones.<br>• Experiencia: Mínima de dos (2) años en operación NOC.<br>• Certificaciones: CompTIA Network+ o equivalente; fabricante del orquestador SD-WAN.<br>• Responsabilidades: Monitorear consolas; triage de alarmas; ejecutar runbooks; escalar; documentar.<br>• Disponibilidad: 24×7 presencial en turnos.<br>• Personal de planta: Sí. |
| **P3. Perfiles técnicos de Seguridad** | **P3.1.** | **Analistas de Seguridad N1**<br>• Objeto y rol: Monitoreo de eventos de seguridad y triage inicial 24×7 en el SOC.<br>• Cantidad mínima: seis (6), en turnos 7×24. Dedicación: 100 %. Periodo: treinta y seis (36) |

| | |
|---|---|
| | meses.<br>• Estudios: Tecnólogo o profesional en Sistemas/afines.<br>• Experiencia: Mínima de dos (2) años en SOC o monitoreo de seguridad.<br>• Certificaciones: Curso CompTIA Security+ o equivalente; preferiblemente del fabricante SIEM.<br>• Responsabilidades: Monitorear consolas SIEM; ejecutar runbooks de triage; escalar a N2 conforme matriz de severidad; cerrar casos S3/S4; documentar evidencias.<br>• Disponibilidad: 24×7 en turnos.<br>• Personal de planta: Sí (PROVEEDOR, filial o aliado autorizado).<br><br>**P3.2. Analistas de Respuesta a Incidentes N2**<br>• Objeto y rol: Análisis profundo, contención y erradicación de incidentes de seguridad.<br>• Cantidad mínima: cuatro (4). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Profesional en Sistemas/Telecomunicaciones; deseable especialización en seguridad.<br>• Experiencia: Mínima de cuatro (4) años en respuesta a incidentes.<br>• Certificaciones: Una (1) de las siguientes: GIAC GCIH, GIAC GCFA, EC-Council ECIH, CompTIA CySA+ o equivalente.<br>• Responsabilidades: Análisis forense en vivo; ejecución de playbooks; coordinación con N3 y fabricantes; emisión de informes de causa raíz; gestión de incidentes S1/S2.<br>• Disponibilidad: 5×8 + guardia 24×7.<br>• Personal de planta: Sí.<br><br>**P3.3. Operadores de Seguridad**<br>• Objeto y rol: Operación cotidiana de plataformas de seguridad (NGFW, WAF, DDoS, antimalware).<br>• Cantidad mínima: cuatro (4). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Tecnólogo en Sistemas/afines.<br>• Experiencia: Mínima de dos (2) años en operación de plataformas de seguridad.<br>• Certificaciones: Del fabricante operado; CompTIA Security+ mínimo.<br>• Responsabilidades: Ejecutar cambios aprobados; backup de configuraciones; aplicar parches; monitorear plataformas; reportar incidentes.<br>• Disponibilidad: 5×8 presencial con turnos extendidos según necesidad operacional. |

| | |
|---|---|
| | • Personal de planta: Sí.<br><br>**P3.4. Administrador Endpoint (Antimalware/XDR)**<br>• Objeto y rol: Administración de la plataforma de protección de endpoints y XDR.<br>• Cantidad mínima: uno (1). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Profesional en Sistemas/afines.<br>• Experiencia: Mínima de tres (3) años administrando plataformas EDR/XDR.<br>• Certificaciones: Del fabricante de la plataforma EDR/XDR ofertada.<br>• Responsabilidades: Despliegue de agentes; políticas; cuarentenas; integración con SOC; respuesta a alertas; reportes mensuales de cobertura.<br>• Disponibilidad: 5×8 + guardia para incidentes P1.<br>• Personal de planta: Sí.<br><br>**P3.5. Ingeniero DevSecOps**<br>• Objeto y rol: Automatización SOAR, integración con CI/CD de seguridad, mantenimiento de playbooks.<br>• Cantidad mínima: uno (1). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Profesional en Sistemas/Telecomunicaciones.<br>• Experiencia: Mínima de tres (3) años en DevSecOps; experiencia en SOAR.<br>• Certificaciones: Del fabricante SOAR; certificación de plataforma de orquestación.<br>• Responsabilidades: Diseñar y mantener playbooks SOAR; integraciones API; automatización de respuesta; aprovisionamiento como código de políticas de seguridad.<br>• Disponibilidad: 5×8 presencial de lunes a viernes durante toda la ejecución del contrato, con disponibilidad adicional cuando la operación lo requiera.<br>• Personal de planta: Sí.<br><br>**P3.6. Analista SOC N3 — Respuesta a incidentes y forensia digital**<br>• Objeto y rol: Tercer nivel de respuesta a incidentes de seguridad, análisis forense digital y determinación de causa raíz de los incidentes de severidad S1 y S2.<br>• Cantidad mínima: dos (2). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Profesional en Ingeniería de Sistemas, Telecomunicaciones o afines; deseable posgrado en seguridad de la |

| | | |
|---|---|---|
| | | información o en informática forense.<br>• Experiencia: Mínima de seis (6) años de experiencia profesional y tres (3) años de experiencia específica en respuesta a incidentes y análisis forense digital.<br>• Certificaciones: GCFA, GCFE, GREM, CHFI o certificaciones equivalentes que acrediten las mismas competencias del rol; certificación vigente del fabricante del SIEM efectivamente ofertado, o equivalente.<br>• Responsabilidades: Atender los incidentes escalados por el nivel N2; ejecutar la adquisición y el análisis forense preservando la cadena de custodia; elaborar los informes de causa raíz; determinar el alcance y la contención definitiva de los incidentes mayores; atender los requerimientos probatorios que formule la Entidad; mantener actualizados los procedimientos forenses y de manejo de evidencia; participar en las mesas de crisis.<br>• Disponibilidad: 5×8 con guardia 24×7 para incidentes de severidad S1 y S2.<br>• Modalidad: presencial durante toda la ejecución del contrato, con disponibilidad adicional cuando la operación lo requiera.<br><br>• Personal de planta: Sí. |
| | **P3.7.** | **Especialista SASE/SSE**<br>• Objeto y rol: Administración y afinamiento de la plataforma SASE/SSE —pasarela web segura, CASB y acceso de red de confianza cero— y de las políticas de acceso seguro para usuarios y sedes.<br>• Cantidad mínima: uno (1). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Profesional en Ingeniería de Sistemas, Telecomunicaciones, Electrónica o afines.<br>• Experiencia: Mínima de cuatro (4) años administrando plataformas de seguridad en producción y dos (2) años específicos en soluciones SASE/SSE o de acceso seguro a internet y aplicaciones.<br>• Certificaciones: Certificación vigente de la solución SASE/SSE efectivamente ofertada, o equivalente; certificación base de seguridad (CISSP, CompTIA Security+ o equivalente).<br>• Responsabilidades: Administrar las políticas de navegación, CASB y acceso de confianza cero; gestionar la inspección TLS y el régimen de excepciones; integrar la plataforma con la identidad institucional y con la red SD-WAN; |

| | |
|---|---|
| | afinar reglas y reducir falsos positivos; controlar la cobertura de usuarios y dispositivos; reportar mensualmente eficacia, capacidad y desviaciones.<br>• Disponibilidad: 5×8 con guardia para incidentes P1.<br>• Personal de planta: Sí.<br><br>**P3.8. Especialista DLP**<br>• Objeto y rol: Administración de la plataforma de prevención de fuga de información (DLP) en correo electrónico, endpoint, nube y navegación.<br>• Cantidad mínima: uno (1). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Profesional en Ingeniería de Sistemas, Telecomunicaciones o afines.<br>• Experiencia: Mínima de cuatro (4) años administrando plataformas de protección de la información y dos (2) años específicos en DLP.<br>• Certificaciones: Certificación vigente de la plataforma DLP efectivamente ofertada, o equivalente; formación acreditada en protección de datos personales conforme a la Ley 1581 de 2012.<br>• Responsabilidades: Construir y afinar las políticas, diccionarios y reglas de clasificación; gestionar el ciclo de vida de los incidentes de fuga de información; coordinar el piloto y el despliegue por olas definidos en el Anexo Técnico 2; reducir falsos positivos; articular la respuesta con el SOC; reportar mensualmente cobertura, incidentes y tendencias.<br>• Disponibilidad: 5×8 con guardia para incidentes P1.<br>• Personal de planta: Sí.<br><br>**P3.9. Especialista NAC**<br>• Objeto y rol: Administración del control de acceso a la red (NAC) y de las políticas de autenticación y de postura de los dispositivos que se conectan a la red institucional.<br>• Cantidad mínima: uno (1). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Profesional en Ingeniería de Sistemas, Telecomunicaciones, Electrónica o afines.<br>• Experiencia: Mínima de cuatro (4) años en operación de redes y dos (2) años específicos en plataformas de control de acceso a la red.<br>• Certificaciones: Certificación vigente de la plataforma NAC en operación en la Entidad o de la efectivamente ofertada, o certificación equivalente que acredite las mismas |

competencias del rol.
• Responsabilidades: Administrar las políticas de autenticación 802.1X y de autenticación por dirección física; gestionar el perfilamiento y la evaluación de postura de los dispositivos; integrar el NAC con la identidad institucional y con la infraestructura LAN; atender los incidentes de acceso a la red; mantener el inventario de dispositivos autorizados y el registro de excepciones; reportar mensualmente cobertura, excepciones y bloqueos.
• Disponibilidad: 5×8 con disponibilidad adicional durante ventanas de mantenimiento y cambios programados.
• Personal de planta: Sí.

**P3.10. Especialista PAM**
• Objeto y rol: Administración de la plataforma de gestión de accesos privilegiados (PAM) y custodia de las credenciales de administración de los servicios contratados.
• Cantidad mínima: uno (1). Dedicación: 100 %. Periodo: treinta y seis (36) meses.
• Estudios: Profesional en Ingeniería de Sistemas, Telecomunicaciones o afines.
• Experiencia: Mínima de cuatro (4) años en administración de plataformas de seguridad y dos (2) años específicos en gestión de accesos privilegiados o de identidades.
• Certificaciones: Certificación vigente de la plataforma PAM efectivamente ofertada, o equivalente; certificación base de seguridad (CISSP, CompTIA Security+ o equivalente).
• Responsabilidades: Administrar las bóvedas, la rotación y la custodia de credenciales privilegiadas; configurar y auditar la grabación de sesiones privilegiadas; aplicar el principio de mínimo privilegio y los esquemas de acceso justo a tiempo; tramitar y documentar las solicitudes de acceso excepcional; entregar las evidencias requeridas en auditoría; reportar mensualmente el inventario de cuentas privilegiadas y los accesos ejecutados.
• Disponibilidad: 5×8 con guardia para incidentes P1.
• Personal de planta: Sí.

**P3.11. Pentester / Ethical Hacker**
• Objeto y rol: Ejecución de las pruebas de penetración internas y externas y de las pruebas de penetración persistente definidas en el Anexo Técnico 2.
• Cantidad mínima: uno (1). Dedicación: 50 %.

| | | |
|---|---|---|
| | | Periodo: treinta y seis (36) meses.<br>• Estudios: Profesional en Ingeniería de Sistemas, Telecomunicaciones o afines.<br>• Experiencia: Mínima de cuatro (4) años de experiencia profesional y tres (3) años de experiencia específica en pruebas de penetración y seguridad ofensiva.<br>• Certificaciones: OSCP, GPEN, CEH Practical o certificaciones equivalentes que acrediten las mismas competencias del rol.<br>• Responsabilidades: Planear y ejecutar las campañas de pruebas de penetración conforme al alcance y a la periodicidad definidos en el Anexo Técnico 2; documentar los hallazgos con evidencia reproducible y clasificación de severidad; recomendar la remediación y verificar su cierre efectivo; entregar el informe ejecutivo y el informe técnico de cada campaña; preservar la confidencialidad y la trazabilidad de las pruebas y de la información obtenida.<br>• Disponibilidad: 5×8, conforme al cronograma de campañas acordado con la Entidad.<br>• Personal de planta: Sí. |
| **P4. Perfiles técnicos de Servicios (Mesa de Ayuda y Observabilidad)** | **P4.1.** | **Agentes de Mesa de Ayuda**<br>• Objeto y rol: Mesa de Ayuda / Soporte Operativo Nivel I y apoyo a Nivel II para los servicios de conectividad, seguridad y videoconferencia.<br>• Cantidad mínima: dieciocho (18) —doce (12) de Nivel I y seis (6) de Nivel II—. Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Tecnólogo en áreas afines.<br>• Experiencia: Mínima de dos (2) años en soporte y atención de servicios TIC.<br>• Certificaciones: Certificaciones vigentes del fabricante o de las plataformas provistas en la solución, a presentar dentro de los primeros tres (3) meses de ejecución del contrato.<br>• Responsabilidades: Recibir, registrar y gestionar incidentes y requerimientos; registrar/actualizar/cerrar casos en la herramienta ITSM institucional; acceder y operar plataformas de gestión, monitoreo y administración; coordinar personal técnico en sitio; verificar el estado de canales y servicios con el fin de correlacionar los reportes de los usuarios —el monitoreo proactivo de la plataforma es responsabilidad exclusiva del NOC—; diagnóstico inicial; escalar oportunamente; mantener comunicación con usuarios y Supervisor del Contrato; apoyar |

| | |
|---|---|
| | reportes operativos.<br>• Disponibilidad: 7×14 presencial en sitio (lunes a domingo, turnos de 8 h, incluyendo fines de semana y festivos).<br>• Personal de planta: Sí (PROVEEDOR, filial o aliado autorizado).<br><br>**P4.2. Especialista en Observabilidad**<br>• Objeto y rol: Integración técnica de los servicios contratados con la plataforma de Observabilidad institucional, la cual es de propiedad y responsabilidad de la Entidad y no hace parte del alcance del presente proceso.<br>• Cantidad mínima: uno (1). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Profesional o tecnólogo senior en Sistemas/Telecomunicaciones.<br>• Experiencia: Mínima de cinco (5) años en observabilidad/monitorización; dos (2) años integrando alertas con ITSM y fuentes de seguridad (SIEM/SOC).<br>• Certificaciones: Certificación en la plataforma de Observabilidad institucional o en herramientas de observabilidad equivalentes; ITIL v4.<br>• Responsabilidades: Configurar conectores hacia Observabilidad institucional; mantener calidad de alertas; reducir ruido; informar a ITSM de incidencias; entregar dashboards operativos.<br>• Disponibilidad: 5×8.<br>• Personal de planta: Sí.<br><br>**P4.3. Técnicos de Soporte en Sitio**<br>• Objeto y rol: Atención presencial de incidentes y requerimientos en las sedes y apoyo a la Mesa de Ayuda en las actividades que exigen intervención física sobre los equipos y el cableado.<br>• Cantidad mínima: ocho (8). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Técnico o tecnólogo en Sistemas, Telecomunicaciones, Electrónica o afines.<br>• Experiencia: Mínima de dos (2) años en soporte técnico presencial de servicios TIC.<br>• Certificaciones: ITIL Foundation o equivalente; certificaciones vigentes del fabricante o de las plataformas provistas en la solución, a presentar dentro de los primeros tres (3) meses de ejecución del contrato.<br>• Responsabilidades: Atender presencialmente los incidentes y requerimientos escalados por la Mesa de Ayuda; ejecutar movimientos, |

| | |
|---|---|
| | adiciones y cambios (IMAC); verificar el estado físico de los equipos, del cableado y de los centros de cableado en sede; apoyar las ventanas de mantenimiento y los cortes de la transición; registrar la totalidad de la gestión en la herramienta ITSM institucional; levantar evidencia fotográfica y actas de atención por sede.<br>• Disponibilidad: 5×8 presencial, con disponibilidad adicional durante ventanas de mantenimiento y eventos de alto impacto.<br>• Personal de planta: Sí (PROVEEDOR, filial o aliado autorizado).<br>• Ubicación: Regionales Nororiental, Caribe, Central, Centro Sur, Pacífico, Noroccidental, Eje Cafetero y Orinoquia, con ubicación en las ciudades principales.<br>Nota: La Fiscalía General de la Nación se reserva la facultad de reubicar a cualquiera de los técnicos en las diferentes ciudades capitales del país, de acuerdo con las necesidades del servicio y de la Entidad. Dicha reubicación será informada al contratista con una antelación mínima de dos (2) meses. |
| **P5. Perfiles técnicos de Videoconferencia** | **P5.1. Agentes de Videoconferencia**<br>• Objeto y rol: Operación cotidiana de la plataforma UCaaS y atención a usuarios de salas y eventos.<br>• Cantidad mínima: tres (3). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Tecnólogo o profesional en Producción Audiovisual, Comunicación Audiovisual, Medios Audiovisuales, Producción Multimedia, Ingeniería de Sistemas o carreras afines.<br>• Experiencia: Mínima de dos (2) años en operación de plataformas de videoconferencia.<br>• Certificaciones: Certificación técnica vigente emitida por el fabricante de la plataforma UCaaS ofertada, relacionada con la administración, operación o soporte de la solución propuesta.<br>• Responsabilidades: Agendamiento de eventos; soporte a usuarios; verificación preevento; grabación; monitoreo durante eventos críticos.<br>• Disponibilidad: 5×8 + extensiones según agenda de eventos.<br>• Personal de planta: Sí (PROVEEDOR, filial, empresa del mismo grupo empresarial o aliado autorizado). |

| | |
|---|---|
| | **P5.2. Operador de Sala VC**<br>• Objeto y rol: Operación de salas de videoconferencia tipo DJT, auditorios y eventos especiales (presencial en eventos críticos).<br>• Cantidad mínima: dos (2). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Tecnólogo en Electrónica, Sistemas, Audiovisuales o carreras afines.<br>• Experiencia: Mínima de dos (2) años en operación AV/videoconferencia profesional.<br>• Certificaciones: Certificación técnica vigente emitida por el fabricante de la plataforma UCaaS ofertada o de la solución de videoconferencia propuesta, relacionada con operación, soporte o administración de dispositivos, salas o plataformas de colaboración.<br>• Responsabilidades: Operación técnica de salas durante eventos; verificación de equipos preevento; soporte presencial; coordinación con plataforma UCaaS.<br>• Disponibilidad: Conforme a la agenda de eventos; presencial en auditorios DJT y sedes principales. El PROVEEDOR deberá garantizar el acompañamiento técnico de cada evento presencial programado que lo requiera, incluida la atención de eventos simultáneos en distintas ciudades. Esta exigencia corresponde a la garantía de acompañamiento del evento y no establece una cantidad fija de personal permanente en cada ciudad; los recursos adicionales que el PROVEEDOR disponga para atender picos o simultaneidad no generan costo adicional para la Entidad.<br>• Personal de planta: Sí (PROVEEDOR, filial, empresa del mismo grupo empresarial o aliado autorizado). |
| **P6. Perfiles técnicos de Cableado** | **P6.1. Líder de Cableado certificado**<br>• Objeto y rol: Liderazgo técnico de cuadrillas de cableado estructurado en sede.<br>• Cantidad mínima: seis (6). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Tecnólogo o profesional en Telecomunicaciones/Electrónica/afines.<br>• Experiencia: Mínima de cinco (5) años en cableado estructurado.<br>• Certificaciones: Certificación vigente de cableado estructurado (ANSI/TIA o del fabricante del cableado ofertado).<br>• Responsabilidades: Liderar la cuadrilla; verificar instalación conforme a normativa; |

| | |
|---|---|
| | certificar puntos; entregar informes técnicos por sede.<br>• Disponibilidad: 5×8 según cronograma de instalaciones.<br>• Personal de planta: Sí.<br><br>**P6.2. Eléctrico con certificación CONTE**<br>• Objeto y rol: Ejecución de instalaciones eléctricas asociadas al cableado.<br>• Cantidad mínima: seis (6). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Técnico/tecnólogo en electricidad/electrónica.<br>• Experiencia: Mínima de tres (3) años en instalaciones eléctricas de baja tensión.<br>• Certificaciones: CONTE vigente; curso de trabajo en alturas vigente.<br>• Responsabilidades: Instalación de acometidas, tomas reguladas y normales; coordinación con tableros de distribución; cumplimiento RETIE.<br>• Disponibilidad: 5×8 según cronograma.<br>• Personal de planta: Sí.<br><br>**P6.3. Técnico de Cableado**<br>• Objeto y rol: Ejecución de instalaciones de cableado estructurado y eléctricas básicas.<br>• Cantidad mínima: dieciocho (18). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Técnico en cableado estructurado o telecomunicaciones.<br>• Experiencia: Mínima de dos (2) años en instalaciones de cableado.<br>• Certificaciones: Certificación en cableado estructurado vigente; conocimientos certificados en electricidad; curso de alturas vigente.<br>• Responsabilidades: Tendido de cable, marquillado, certificación de puntos, instalación de canaletas/ductерías, apoyo al Líder.<br>• Disponibilidad: 5×8 según cronograma.<br>• Personal de planta: Sí.<br><br>**P6.4. Ingeniero Líder RCDD/ATD**<br>• Objeto y rol: Auditoría técnica de actividades de cableado en sedes mayores a cien (100) puntos.<br>• Cantidad mínima: uno (1). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Ingeniero en Telecomunicaciones/Electrónica.<br>• Experiencia: Mínima de ocho (8) años en cableado estructurado.<br>• Certificaciones: RCDD (Registered Communications Distribution Designer) o ATD |

| | | |
|---|---|---|
| | | (Approved Technical Designer) vigente, o certificaciones equivalentes que demuestren competencias especializadas en diseño, arquitectura, auditoría o validación de infraestructura de cableado estructurado y telecomunicaciones, siempre que el oferente acredite de manera objetiva la equivalencia funcional de la certificación presentada frente a las responsabilidades definidas para el perfil. La equivalencia deberá presentarse dirigida a la Entidad, al momento de iniciar el contrato con indicación del nombre del proceso y numerto de contrato y con fecha de expedición no mayor a treinta (30) días anteriores a la fecha de inicio del contrato. . La Entidad verificará que la certificación aportada tenga relación directa con las funciones de diseño y auditoría de cableado estructurado exigidas para el rol y podrá solicitar la documentación soporte necesaria para validar dicha equivalencia.<br>• Responsabilidades: Auditar instalación; hacer presencia en sedes mayores a 100 puntos; entregar informes de auditoría con visto bueno; recomendaciones técnicas.<br>• Disponibilidad: Por sede; según cronograma.<br>• Personal de planta: Sí (del fabricante o aliado).<br><br>**P6.5. Coordinador de Implementación Regional**<br>• Objeto y rol: Coordinación logística y técnica de la implementación de cableado a nivel nacional (876 sedes, múltiples regionales).<br>• Cantidad mínima: uno (1). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Profesional en Ingeniería de Sistemas/Telecomunicaciones/Industrial/Eléctrica.<br>• Experiencia: Mínima de cinco (5) años en gestión de proyectos de despliegue nacional.<br>• Certificaciones: PMP o equivalente; conocimientos de cableado estructurado.<br>• Responsabilidades: Coordinar cronograma nacional; gestionar cuadrillas regionales; coordinar con analistas seccionales de la FGN; consolidar entregables; reportar avance regional al Gerente de Proyecto.<br>• Disponibilidad: 5×8 con desplazamientos a regional.<br>• Personal de planta: Sí. |
| **P7. Perfiles de Infraestructura** | **P7.1.** | **Especialistas Linux**<br>• Objeto y rol: Administración, operación y optimización de plataformas Linux (RedHat, Ubuntu) en ambientes productivos y no |

| | |
|---|---|
| | productivos del centro de datos.<br>• Cantidad mínima: dos (2). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Profesional en Ingeniería de Sistemas, Electrónica, Telecomunicaciones o afines.<br>• Experiencia: Mínima de cinco (5) años en administración de sistemas Linux en entornos empresariales, incluyendo administración de servidores físicos y virtuales.<br>• Certificaciones: RHCSA o RHCE vigente; ycertificación Linux Professional Institute (LPIC) o equivalente.<br>• Responsabilidades: Administración de servidores Linux, parchado, monitoreo, automatización, soporte de incidentes, documentación.<br>• Disponibilidad: 5×8 presencial de lunes a viernes durante toda la ejecución del contrato con disponibilidad extendida cuando la operación lo requiera.<br>• Personal de planta: Sí<br><br>**P7.2. Especialistas Plataforma Microsoft**<br>• Objeto y rol: Administración de plataformas Microsoft (Windows Server, Active Directory, servicios asociados y virtualización).<br>• Cantidad mínima: dos (2). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Profesional en Ingeniería de Sistemas o afines.<br>• Experiencia: Mínima de cinco (5) años en administración de productos Microsoft empresariales.<br>• Certificaciones: Microsoft Certified (Azure Administrator / Windows Server / Exchange / DevOps o equivalente).<br>• Responsabilidades: Administración de Windows Server, AD, virtualización, parches, soporte.<br>• Disponibilidad: 5x8 presencial de lunes a viernes durante toda la ejecución del contrato con disponibilidad extendida cuando la operación lo requiera..<br>• Personal de planta: Sí<br><br>**P7.3. Especialista de Almacenamiento**<br>• Objeto y rol: Gestión integral de plataformas de almacenamiento empresarial HITACHI VANTARA.<br>• Cantidad mínima: uno (1). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Profesional en Ingeniería de |

| | |
|---|---|
| | Sistemas o afines.<br>• Experiencia: Mínima de cinco (5) años en SAN/NAS y backup de centro de datos.<br>• Certificaciones: Certificación vigente del fabricante de las plataformas de almacenamiento y respaldo en operación en la Entidad, o certificación equivalente que acredite las mismas competencias del rol.<br>• Responsabilidades: Administración, tuning, backups, seguridad, documentación.<br>• Disponibilidad: 5×8 presencial de lunes a viernes durante toda la ejecución del contrato con disponibilidad extendida cuando la operación lo requiera..<br>• Personal de planta: Sí<br><br>**P7.4. Especialista DBA**<br>• Objeto y rol: Administración de bases de datos<br>• Cantidad mínima: uno (1). Dedicación: 100 %. Periodo: treinta y seis (36) meses.<br>• Estudios: Profesional en Ingeniería de Sistemas o afines.<br>• Experiencia: Mínima de cinco (5) años en administración de bases de datos Sql Server, Oracle, MySql, MariaDB, Postgres.<br>• Certificaciones: Certificación vigente de administración de bases de datos, nivel asociado o profesional, del fabricante de los motores en operación en la Entidad, o certificación equivalente que acredite las mismas competencias del rol.<br>• Responsabilidades: administración, optimización, backups, seguridad y documentación<br>• Disponibilidad: 5×8 presencial de lunes a viernes durante toda la ejecución del contrato con disponibilidad extendida cuando la operación lo requiera..<br>• Personal de planta: Sí<br><br>**P7.5. Operadores de Centro de Datos**<br>• Objeto y rol: Operación técnica y soporte de la infraestructura física de los centros de datos de la Fiscalía General de la Nación.<br>• Cantidad mínima: cuatro (4), en turnos rotativos para la cobertura 7×24. Dedicación: 100 % presencial. Periodo: treinta y seis (36) meses.<br>• Estudios: Minimo tecnólogo en sistemas, redes o telecomunicaciones.<br>• Experiencia: Mínima de tres (3) años en centros de datos TIER 2 o superior.<br>• Certificaciones: Redes o DataCenter. |

| | |
|---|---|
| | • Responsabilidades: Monitoreo, cableado, soporte, inventarios, apoyo.<br>• Disponibilidad: 7x24 presencial durante toda la ejecución del contrato, con disponibilidad adicional cuando la operación lo requiera.<br>• Personal de planta: Sí |

P8. Entregables mensuales consolidados por perfil

Cada perfil técnico debe entregar mensualmente diez (10) productos como mínimo. Los entregables son exigibles por categoría o rol y se presentan de manera consolidada por el equipo del rol —no por cada persona individualmente asignada—, sin perjuicio de que la información se desagregue por sede, cuadrilla o evento cuando la naturaleza del entregable lo exija, conforme a los formatos que defina la Entidad. La siguiente tabla consolida los entregables por categoría:

| Categoría | Entregables mensuales mínimos (10 por perfil) |
|---|---|
| **Roles estratégicos (P1)** | (1) Informe ejecutivo mensual; (2) Acta de comité técnico; (3) Indicadores ANS T. ANS Transversales y plan de mejora; (4) Informe de cambios mayores; (5) Informe de incidentes mayores y RCAs; (6) Inventario actualizado de activos críticos; (7) Roadmap de fabricantes; (8) Plan mensual de continuidad y HA/DR; (9) Estado de la integración entre dominios; (10) Recomendaciones accionables a la FGN. |
| **Conectividad (P2)** | (1) ANS de C. Conectividad por servicio, por categoría de sede donde aplique, por mes; (2) Informe de saturación y capacidad; (3) RCAs de incidencias mayores; (4) Control de cambios RFC; (5) Inventario de enlaces; (6) Pruebas técnicas PAT; (7) Estado de QoS/clases de servicio; (8) Reporte de escalamiento a carriers/ISP; (9) Topologías actualizadas; (10) Plan mensual de optimización. |
| **Seguridad (P3)** | (1) Cambios de políticas/reglas; (2) Eficacia de detecciones y falsos positivos; (3) Hallazgos y remediación de vulnerabilidades; (4) Disponibilidad/capacidad de plataformas de seguridad; (5) Análisis de amenazas detectadas; (6) Pruebas funcionales de control; (7) Inventario de activos protegidos; (8) Reporte de cumplimiento de hardening; (9) Mapa de riesgos actualizado; (10) Plan mensual de mejora. |
| **Servicios (P4)** | (1) Reporte de productividad de mesa; (2) Calidad de tickets (auditoría); (3) Cuadrantes de turnos y cobertura; (4) Escalamientos y causas; (5) Top 10 causas raíz operativas; (6) Actualización de base de conocimiento; (7) Satisfacción/experiencia usuario; (8) Cambios menores ejecutados; (9) Acta de comité |

| | |
|---|---|
| | mensual; (10) Plan mensual de formación. |
| **Videoconferencia (P5)** | (1) Eventos atendidos y agendados; (2) Disponibilidad de salas; (3) Calidad técnica de eventos (jitter, latencia, mosaicos); (4) Incidentes mayores; (5) Inventario de equipos por sala; (6) Control de licencias; (7) Soporte a webinars masivos; (8) Actualizaciones de plataforma; (9) Integración con Teams; (10) Plan mensual de mejora. |
| **Cableado (P6)** | (1) Avance del cronograma nacional; (2) Puntos certificados; (3) Reporte fotográfico por sede; (4) Cumplimiento normativa ANSI/TIA, RETIE, NTC 2050; (5) Inventario de materiales; (6) Garantías por sede; (7) Coordinación con analistas seccionales FGN; (8) Riesgos y mitigaciones; (9) Acta de comité regional; (10) Plan mensual de implementación. |
| **Infraestructura (P7)** | (1) Informe técnico mensual consolidado de la plataforma o componente administrado (estado, disponibilidad, eventos relevantes); (2) Reporte mensual de incidentes gestionados, incluyendo clasificación, severidad, tiempos de atención y estado de cierre; (3) Análisis de incidentes relevantes con causa raíz (RCA), únicamente para eventos de impacto significativo; (4) Reporte de cambios ejecutados mediante RFC, incluyendo validación, ventana de ejecución y resultado; (5) Informe de monitoreo de capacidad y desempeño de la plataforma (uso de recursos, tendencias, alertas); (6) Inventario técnico actualizado de componentes bajo su administración (servidores, instancias, bases de datos, contenedores, volúmenes, etc.); (7) Informe de actividades de mantenimiento realizadas (parches, upgrades, hardening, afinamientos); (8) Reporte del estado de respaldos, replicación o mecanismos de alta disponibilidad aplicables al componente administrado; (9) Actualización de documentación técnica (procedimientos, configuraciones, diagramas o guías operativas); (10) Recomendaciones técnicas orientadas a optimización, mitigación de riesgos o evolución de la plataforma. |
| **Operación Centro de Datos (P7-DC)** | (1) Informe mensual de operación del centro de datos; (2) Registro de monitoreo diario de condiciones ambientales (temperatura, energía, UPS); (3) Registro de incidentes de infraestructura física; (4) Reporte de actividades de mantenimiento preventivo y correctivo; (5) Inventario actualizado de activos físicos (racks, servidores, cableado); (6) Informe de gestión de cableado y organización de racks; (7) Registro de ingresos/salidas de equipos; (8) Evidencias de ejecución de rutinas operativas; (9) Reporte de soporte a instalaciones y movimientos (IMAC); (10) Recomendaciones de mejora en operación y capacidad física. |

P9. Reglas generales del personal del PROVEEDOR

P9.1. Certificaciones vigentes: Todas las certificaciones de fabricante exigidas en los perfiles deben permanecer vigentes durante toda la ejecución del contrato. La pérdida de una certificación obliga al PROVEEDOR a reemplazar al personal afectado en máximo tres (3) días calendario. Toda certificación enunciada en el presente Anexo mediante denominación comercial de fabricante se entenderá referida a la certificación técnica vigente del fabricante de la solución efectivamente ofertada, en el nivel funcional equivalente, y se admitirán certificaciones equivalentes que acrediten las mismas competencias del rol.

P9.2. Personal de planta: Salvo excepciones expresamente definidas, todo el personal asignado al contrato debe ser personal de planta del PROVEEDOR, su filial o aliado autorizado, con vinculación laboral directa. Se aceptará personal con vinculación laboral directa con empresas del mismo grupo empresarial del PROVEEDOR (matriz, filial o subordinada), siempre que se acredite la relación societaria y el cumplimiento integral de los requisitos de formación, experiencia, certificaciones, disponibilidad y dedicación del perfil. Tratándose de uniones temporales o consorcios, la condición de personal de planta se entiende cumplida con la vinculación laboral directa a cualquiera de sus integrantes, a su filial, a su aliado autorizado o a empresas del mismo grupo empresarial. No se exige antigüedad mínima de vinculación: el personal podrá ser contratado para la ejecución del presente contrato, siempre que acredite los requisitos de formación, experiencia, certificaciones y dedicación definidos para el perfil. No se admite la vinculación mediante contrato de prestación de servicios ni esquemas de dedicación compartida. El objeto contractual corresponde a la prestación de un servicio gestionado integral y no al suministro o intermediación de personal; el PROVEEDOR conserva la autonomía técnica, administrativa y laboral para organizar el equipo, sin que exista vínculo laboral entre la FGN y las personas destinadas a la ejecución, y mantiene en todos los casos la responsabilidad integral por la prestación del servicio, el cumplimiento de los perfiles, la continuidad operativa, los productos y los ANS. Una organización que emplee personas con discapacidad no adquiere por ese solo hecho la condición de aliado autorizado; dicha condición deberá derivarse de una relación técnica o comercial verificable con la solución ofrecida y no podrá utilizarse para trasladar o subcontratar las obligaciones principales del PROVEEDOR. Las personas con discapacidad podrán desempeñar cualquiera de los perfiles del presente anexo para los cuales cumplan los requisitos de formación, experiencia, certificaciones, dedicación y disponibilidad. Cuando el PROVEEDOR haya obtenido puntaje por acreditar trabajadores con discapacidad, deberá mantener durante la ejecución el número de trabajadores que dio lugar a dicho puntaje, lo cual será verificado por la supervisión o interventoría. El presente anexo no establece valores de remuneración mínima por perfil; los valores salariales del Estudio del Sector y del Formato 8 – Oferta Económica son referenciales, y el PROVEEDOR definirá la remuneración y las condiciones de vinculación de su personal bajo su exclusiva responsabilidad, con cumplimiento de las normas laborales, salariales, prestacionales, de seguridad social y parafiscales aplicables, sin perjuicio de la facultad de la FGN de verificar el cumplimiento de los perfiles y el pago de los aportes al sistema de seguridad social y parafiscales del personal destinado al servicio.

P9.3. Rotación máxima permitida: Una (1) rotación máxima por cada doscientas cuarenta (240) horas de servicio por perfil. Toda rotación adicional requiere autorización expresa de la Supervisión del Contrato. La métrica se computa por perfil o rol —no por persona individualmente considerada— a partir de las horas de servicio efectivamente prestadas por el rol en el período; no se computarán como

rotación las novedades derivadas de causas no imputables al PROVEEDOR ni las solicitadas por la Entidad.

P9.4. ANS de asignación inicial: Tiempos máximos para asignar el perfil al servicio, contados a partir del momento en que el perfil sea exigible conforme a la fase o categoría correspondiente del Plan Detallado de Transición, y no necesariamente desde la firma del Acta de Inicio:• Categoría 1: cuatro (4) días calendario• Categoría 2: cuatro (4) días calendario• Categoría 3: ocho (8) días calendario• Categoría 4: doce (12) días calendario• Categoría 5: cuatro (4) días calendario (coordinado con el proveedor cloud)• Categoría 6: según la ficha del servicio activado. La asignación de los perfiles se efectuará de manera escalonada, conforme al Plan Detallado de Transición y a la fase en la que cada perfil deba prestar el servicio; los roles estratégicos transversales se acreditarán al momento de la suscripción del Acta de Inicio, y los perfiles técnicos y operativos podrán acreditarse de manera progresiva, antes de la fase en la cual prestarán el servicio y dentro de los plazos aquí definidos. La acreditación progresiva y los plazos de asignación no son excluyentes; corresponde al PROVEEDOR garantizar la disponibilidad y capacidad de incorporación de los recursos de acuerdo con el cronograma de transición. Los tiempos se aplican por categoría de servicio y no por un número fijo de perfiles en cada corte, garantizando en todo caso las cantidades mínimas del presente anexo. El perfil Gestor de Transición deberá estar disponible desde D-15 y durante los meses uno (1) a diez (10), conforme a su ficha; los perfiles de cableado estructurado (P6) serán exigibles a partir de la activación de las actividades de cableado previstas en el Plan Detallado de Transición, aplicando para su asignación los plazos de la categoría del servicio correspondiente. El tiempo utilizado exclusivamente por la FGN para realizar el estudio de seguridad institucional (P9.7), verificar antecedentes y expedir credenciales no se contabilizará dentro de estos plazos ni se imputará al PROVEEDOR para efectos de este ANS ni de las penalidades del capítulo P del Anexo Técnico 5, siempre que el PROVEEDOR haya presentado oportunamente la documentación completa del candidato y atendido los requerimientos de la Entidad. La medición y las penalidades asociadas a este ANS se rigen exclusivamente por el Anexo Técnico 5 – Acuerdo de Niveles de Servicio (ANS).

P9.5. Reemplazo por novedad: El PROVEEDOR debe asignar reemplazo en máximo tres (3) días calendario ante novedades de personal. El reemplazo debe cumplir los mismos requisitos del perfil. El tiempo utilizado exclusivamente por la FGN para realizar el estudio de seguridad, verificar antecedentes y expedir las credenciales de acceso del reemplazo no se contabilizará dentro de dicho plazo, siempre que el PROVEEDOR haya presentado oportunamente la documentación completa y atendido los requerimientos de la Entidad. Mientras finalizan los controles institucionales, el PROVEEDOR deberá adoptar las medidas de contingencia necesarias para garantizar la continuidad del servicio, y el reemplazo no podrá acceder a información sensible, sistemas o instalaciones restringidas hasta obtener las autorizaciones correspondientes.

P9.6. Cumplimiento Ley 1581 de 2012: Todo el personal debe firmar acuerdo de confidencialidad y cumplimiento de la normativa de protección de datos personales (Ley 1581 de 2012 y normativa asociada).

P9.7. Estudios de seguridad: Todo el personal que tenga acceso a información sensible debe surtir el estudio de seguridad institucional de la FGN, conforme a los procedimientos vigentes. El estudio aplica a todo el personal del PROVEEDOR que, en razón de sus funciones, tenga acceso a información,

sistemas, plataformas o instalaciones restringidas de la Entidad, y comprende, como mínimo, los perfiles con acceso administrativo o privilegiado a las plataformas, los perfiles del SOC y del NOC, y los que presten servicios en los centros de datos o en sedes con restricciones de acceso. El estudio lo realiza directamente la FGN, conforme a sus procedimientos institucionales, sin costo para el PROVEEDOR; los documentos requeridos se informarán al inicio de la ejecución conforme a los formatos institucionales, y su duración dependerá del perfil, el nivel de acceso, la completitud de la documentación y las verificaciones requeridas. Mientras el estudio se surte, el candidato no podrá acceder a información sensible, sistemas ni instalaciones restringidas, y el PROVEEDOR deberá adoptar las medidas de contingencia necesarias para garantizar la continuidad del servicio. Cuando el resultado no sea favorable, la FGN lo informará al PROVEEDOR sin que esté obligada a revelar los motivos, en atención a la reserva de la información y a la protección de datos personales; el PROVEEDOR deberá presentar un nuevo candidato que cumpla integralmente los requisitos del perfil dentro del plazo previsto en el numeral P9.5, contado a partir de la comunicación de la Entidad, y esta sustitución no se considerará rotación de personal en los términos del numeral P9.3.

P9.8. Capacitación inicial obligatoria: Todo el personal debe completar la capacitación inicial sobre las políticas, procedimientos y herramientas de la FGN durante las primeras dos (2) semanas de su asignación. La capacitación inicial no suspende ni amplía los plazos de asignación del numeral P9.4, y el personal podrá iniciar sus actividades mientras la completa.

P9.9. Disponibilidad, guardias y festivos: los esquemas de operación 24×7 o 7×24 "en turnos" corresponden a trabajo activo programado e incluyen la cobertura de fines de semana y días festivos, al igual que el esquema 7×14 en sitio. Las expresiones "guardia", "disponibilidad adicional" o "disponibilidad ampliada" corresponden a disponibilidad bajo llamado para la atención de incidentes críticos, ventanas de mantenimiento, mesas de crisis o eventos de alto impacto, y no configuran una jornada permanente 7×24. La guardia podrá atenderse de forma remota, siempre que se garanticen los tiempos de respuesta y los niveles de servicio exigidos; la guardia no podrá utilizarse como mecanismo permanente para suplir una malla operativa insuficiente. La disponibilidad se acreditará mediante los cuadrantes de turnos y cobertura, entregable mensual de la categoría de Servicios (P4).

P9.10. Contabilización de la experiencia: La experiencia profesional exigida en los perfiles se contabiliza a partir de la fecha de expedición de la tarjeta o matrícula profesional, cuando la profesión la requiera conforme a la normativa aplicable; en los demás casos, a partir de la certificación laboral o académica correspondiente. La experiencia específica de cada rol se acreditará mediante certificaciones de contratos o proyectos en los que se haya ejercido dicho rol.

| | |
|---|---|
| **Empaque y rotulado** | **No aplica. El servicio corresponde a la prestación de servicios profesionales a cargo del PROVEEDOR, medidos por perfil asignado al servicio.** |
| **Presentación y Unidad de Medida** | Cantidad de perfiles asignados al servicio por mes. |

| **Concepto** | **Nombre y apellidos** | **Rol** | **Firma** |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Aprobó | Eric Mauricio Vargas Forero | Jefe Departamento De Infraestructura | |
| Aprobó | Giselle Viviana Muñeton Lara | Coordinadora de Seguridad | |
| Revisó | Carlos Alberto Pinto Chaparro | Estructurador | |
| Revisó | Jorge Eduardo Ariza Carrillo | Estructurador | |
| Revisó | Jose Manuel Rodríguez | Estructurador | |
| Revisó | Joan Andres Perdomo Hernandez | Estructurador | |
| Revisó | Jose Luis Daza Perez | Estructurador | |
| Revisó | Roger Andres Ortiz Tamayo | Estructurador | |
| Revisó | William Andres Angarita Tovar | Estructurador | |
| Revisó | Frankin Leonardo Bermudez Gil | Estructurador | |