1. Resumen Ejecutivo

Este documento detalla el alcance requerido de los servicios profesionales para la implementación, configuración y puesta en marcha de una solución de red y seguridad integral de acuerdo con los requerimientos establecidos en el pliego de condiciones INDOTEL-CCC-LPN-2025-0014. El objetivo es dotar al nuevo edificio 323 de una infraestructura de red moderna, segura, escalable y de alto rendimiento, que sirva como base para todos los servicios tecnológicos de la institución.

El proyecto abarca el despliegue de firewalls de próxima generación, una infraestructura de switching multicapa, una red inalámbrica Wi-Fi 7, y soluciones avanzadas de control de acceso (NAC), seguridad para acceso remoto (SASE), gestión centralizada y reportería. Debido a que en el pliego de condiciones no se estableció el requerimiento especifico de dichos servicios, se establecen a continuación los requerimientos que cada oferente debe cumplir e incluir en su propuesta técnica y económica.

2. Gestión del Proyecto

Se deberá asignar un Gerente de Proyecto certificado que será el punto de contacto principal y responsable de la ejecución exitosa del proyecto.

- Actividades Incluidas:
    - **Reunión de Inicio (Kick-off):** Presentación de los equipos de trabajo, validación de los objetivos, alcance y cronograma del proyecto.
    - **Plan de Trabajo Detallado:** Entrega de un cronograma (Project Plan) con fases, tareas, responsables y fechas de entrega.
    - **Reuniones de Seguimiento:** Se llevarán a cabo reuniones periódicas para revisar avances, identificar riesgos y tomar decisiones.
    - **Documentación del Proyecto:** Entrega de toda la documentación requerida, incluyendo diseño de alto y bajo nivel, diagramas de red y manuales de configuración.

3. Equipo de Proyecto y Perfiles Requeridos

Para garantizar una ejecución de la más alta calidad y en cumplimiento con las mejores prácticas de la industria, el proyecto será implementado por un equipo de profesionales con experiencia comprobada y certificaciones vigentes. El equipo estará conformado por los siguientes roles:

a. Líder Técnico

Será el responsable de dirigir al equipo técnico, validar el diseño de la solución y actuar como el principal interlocutor técnico ante INDOTEL para todos los aspectos del proyecto.

- Perfil Mínimo:

- Graduado como Ingeniero.
- Certificación FCX (Fortinet Certified Expert) o equivalente (CCIE Security, HCIE Security, JNCIE Security, ACCX) vigente y activa.
- Certificado Especialista en soluciones de seguridad de red o equivalente, vigente y activo.
- Certificado en desarrollo aplicado a redes a nivel profesional, vigente y activo.
- Ser empleado a tiempo completo del oferente (se suministrará evidencia de TSS de los últimos 6 meses).
- Experiencia demostrable en un mínimo de tres (3) proyectos similares.

b. Especialista en Redes

Encargado de la implementación, configuración y puesta a punto de toda la infraestructura de switching y la red inalámbrica.

- Perfil Mínimo:
  - Certificación FCX (Fortinet Certified Expert) o equivalente (CCIE, HCIE, JNCIE, ACSX) vigente y activa.
  - Certificación a nivel profesional en seguridad.
  - Ser empleado a tiempo completo del oferente (se suministrará evidencia de TSS de los últimos 6 meses).
  - Experiencia demostrable en un mínimo de tres (3) proyectos similares.

c. Especialista en Seguridad

Responsable de la implementación de los componentes de seguridad perimetral, específicamente los firewalls, y las soluciones de acceso seguro como SASE y NAC.

- Perfil Mínimo:
  - Certificación FCP (Fortinet Certified Professional) o equivalente (CCNP Security, HCIP Security, JNCIP Security, ACSP) vigente y activa.
  - Certificado
    Especialista en soluciones SASE del fabricante ofertado, vigente y activo[55].
  - Certificado Especialista en soluciones de seguridad de red del fabricante ofertado, vigente y activo.
  - Ser empleado a tiempo completo del oferente (se suministrará evidencia de TSS de los últimos 6 meses).
  - Experiencia demostrable en un mínimo de tres (3) proyectos similares.

d. Especialista en Ciberseguridad

Dará soporte en la implementación de los diversos controles de seguridad del proyecto, asegurando el cumplimiento de las políticas y mejores prácticas de ciberseguridad.

- Perfil Mínimo:
  - Certificación FCP (Fortinet Certified Professional) o equivalente (CCNP, HCIP, JNCIP, ACSP) vigente y activa.
  - Certificación CompTIA Security+.
  - Certificación ITIL.

- Ser empleado a tiempo completo del oferente (se suministrará evidencia de TSS de los últimos 6 meses).
- Experiencia demostrable en un mínimo de tres (3) proyectos similares.

4. Alcance de Servicios por Componente

4.1. Firewalls de Próxima Generación (2x Firewalls)

- **Objetivo:** Desplegar una solución de seguridad perimetral redundante que ofrezca protección avanzada contra amenazas, segmentación interna y conectividad WAN segura y optimizada mediante SD-WAN.
- **Fases y Actividades:**
  1. **Diseño y Planificación:**
     - Levantamiento de información sobre la arquitectura de red actual, direccionamiento IP, políticas de seguridad y requerimientos de conectividad.
     - Diseño de la topología de red, incluyendo la configuración de alta disponibilidad (HA) en modo Activo-Pasivo.
     - Diseño de la estrategia de SD-WAN para optimizar el uso de los enlaces de internet y MPLS.
  2. **Instalación y Configuración:**
     - Instalación física (enrackado) y conexión de los dos (2) equipos firewalls.
     - Configuración del clúster de Alta Disponibilidad para garantizar la continuidad del servicio.
     - Configuración de interfaces de red, VLANs, y protocolos de enrutamiento (OSPF, BGP) según se requiera.
     - Creación de políticas de firewall para controlar el tráfico entre las distintas zonas de la red (interna, DMZ, WAN).
     - Habilitación y configuración de los perfiles de seguridad UTM: Antivirus, Prevención de Intrusiones (IPS), Filtrado Web, Control de Aplicaciones y DLP.
     - Configuración de la funcionalidad de SD-WAN, incluyendo reglas de selección de ruta dinámica, medición de la calidad de los enlaces (SLA) y políticas de calidad de servicio (QoS).
  3. **Integración y Pruebas:**
     - Integración con Microsoft Active Directory para la identificación de usuarios y la aplicación de políticas basadas en roles.
     - Configuración del envío de logs hacia la solución de reportería y almacenamiento de logs.
     - Registro de los equipos en la solución Central Management para su gestión centralizada.

        - Realización de pruebas de validación de conectividad, aplicación de políticas y conmutación por error (failover) del clúster HA.
    4. **Documentación y Transferencia de Conocimiento:**
        - Entrega de diagramas de red "as-built" y documentación detallada de la configuración.
        - Sesión de transferencia de conocimiento al personal técnico de INDOTEL sobre la gestión y monitoreo de la solución.

4.2. Infraestructura de Switching (60x switches)

- **Objetivo:** Implementar una infraestructura de switching segura, resiliente y gestionada de forma centralizada, que proporcione conectividad de alta velocidad en las capas de acceso, distribución y núcleo de la red.
- **Fases y Actividades:**
    1. **Diseño y Planificación:**
        - Diseño de la arquitectura de switching, definiendo los roles de cada equipo (Núcleo: 2x, Acceso: 32x 24 puertos, 20x 48 puertos, 6x 48 puertos FPOE).
        - Planificación del esquema de VLANs y segmentación de la red.
        - Diseño de la agregación de enlaces (LACP) para los puertos de uplink y la interconexión del núcleo.
    2. **Instalación y Configuración:**
        - Instalación física (enrackado) de los sesenta (60) switches.
        - Configuración de los dos (2) switches de núcleo (FS-1048E) en modo MCLAG (Multi-Chassis Link Aggregation) para redundancia a nivel de chasis.
        - Configuración de enlaces en los firewalls para la gestión centralizada de todos los switches.
        - Aprovisionamiento de VLANs, políticas de PoE/PoE+/PoE++ en los puertos de acceso para alimentar Access Points y otros dispositivos.
        - Implementación de políticas de seguridad a nivel de puerto: DHCP Snooping, Dynamic ARP Inspection, y Control de Tormentas.
    3. **Integración y Pruebas:**
        - Integración con la solución NAC para la aplicación de políticas de control de acceso dinámico en los puertos.
        - Validación de la conectividad de Capa 2 y Capa 3 en toda la infraestructura.
        - Pruebas de redundancia y convergencia de la red ante fallos de enlaces o equipos.
    4. **Documentación y Transferencia de Conocimiento:**
        - Entrega de documentación con el direccionamiento, configuración de puertos y VLANs.
        - Sesión de capacitación sobre la administración de los switches desde la consola del firewall.

4.3. Red Inalámbrica (60x AP Wi-Fi 7)

- **Objetivo:** Desplegar una red inalámbrica de última generación (Wi-Fi 7) que ofrezca cobertura total, alta densidad de usuarios y acceso seguro y diferenciado para empleados e invitados.
- **Fases y Actividades:**
    1. **Diseño y Planificación:**
        - Validación de las ubicaciones de los 60 Access Points (37x densidad media y 23x densidad alta) para una cobertura óptima.
        - Diseño de los SSIDs (identificadores de red), incluyendo red corporativa, red de invitados y redes para propósitos especiales.
        - Definición de las políticas de autenticación: WPA3-Enterprise con 802.1X para la red corporativa y portal cautivo para la red de invitados.
    2. **Instalación y Configuración:**
        - Coordinación de la instalación física de los 60 APs.
        - Configuración del controlador inalámbrico integrado en los FortiGate para gestionar todos los APs.
        - Creación de los SSIDs con sus respectivos métodos de seguridad, asignación de VLANs y perfiles de QoS.
        - Configuración del portal cautivo para el acceso de invitados.
    3. **Integración y Pruebas:**
        - Integración con un servidor RADIUS (o el servicio de NAC) para la autenticación 802.1X de usuarios corporativos.
        - Aplicación de políticas de firewall específicas para cada SSID en el firewall.
        - Realización de pruebas de cobertura, rendimiento, roaming entre APs y conectividad de los clientes.
    4. **Documentación y Transferencia de Conocimiento:**
        - Entrega de documentación sobre la configuración de la red inalámbrica y el portal de invitados.
        - Capacitación al equipo de INDOTEL sobre el monitoreo de la salud de la red Wi-Fi y la gestión de clientes.

4.4. Soluciones Centralizadas y de Acceso Seguro

- **Objetivo:** Implementar un conjunto de soluciones para centralizar la gestión, el análisis de logs, el control de acceso a la red y la seguridad de usuarios remotos, creando un ecosistema de seguridad integrado y automatizado.
- **Fases y Actividades:**
    1. **Gestión Centralizada:**
        - Despliegue de la máquina virtual de la solución de gestión centralizada.

- Añadir el clúster de firewall para su gestión, creando un ADOM (Dominio Administrativo).
- Configuración de plantillas y scripts para estandarizar configuraciones.
- Capacitación sobre el uso de la solución de gestión centralizada para desplegar políticas y realizar cambios de forma centralizada.

2. Reportería y Almacenamiento de Logs:
   - Despliegue de la máquina virtual de reportería y almacenamiento de logs.
   - Configuración de todos los equipos propuestos (firewall, Switch, AP) para enviar logs a la solución de reportería y almacenamiento de logs.
   - Personalización de dashboards y reportes para visibilidad del tráfico, amenazas y cumplimiento normativo (PCI DSS).
   - Configuración de alertas automáticas para eventos críticos de seguridad.
3. Control de Acceso a la Red:
   - Despliegue de la máquina virtual de NAC.
   - Integración con la infraestructura de red (firewall, Switch) y con Active Directory.
   - Configuración de políticas de perfilamiento para descubrir y clasificar automáticamente todos los dispositivos que se conectan a la red (PCs, IoT, móviles).
   - Creación de políticas de control de acceso basadas en roles para segmentar y aislar dispositivos según su perfil y nivel de cumplimiento.
   - Implementación de la respuesta automatizada para poner en cuarentena dispositivos no conformes o sospechosos.
4. Solución Secure Access Service Edge:
   - Activación y configuración del portal de SASE para 200 usuarios.
   - Configuración del agente unificado para el acceso seguro a Internet (SWG), a aplicaciones en la nube (CASB) y a la red interna (ZTNA).
   - Establecimiento del conector SD-WAN en los firewall para un acceso privado seguro desde los usuarios remotos hacia las aplicaciones del centro de datos.
   - Creación de políticas de seguridad consistentes para usuarios dentro y fuera de la oficina.

5. Entrega Final y Aceptación

Al finalizar la implementación de todos los componentes, se deberá realizar una fase de validación final junto con el equipo técnico de INDOTEL. Se deberá ejecutar un conjunto de pruebas de aceptación (UAT) para confirmar que la solución cumple con todos los requerimientos funcionales y de rendimiento especificados. Una vez superadas las pruebas, se procederá a firmar el acta de conformidad y se aceptará la entrega formal del proyecto.