Solicitud No.			TIC-INT-69-25
Fecha:	04	07	2025

Nombre del Bien/Servicio	***Dispositivos de Autenticación Multifactor (MFA): YubiKey u otros compatibles FIDO2***
Descripción y Uso	Es un dispositivo que refuerza la seguridad de las cuentas de usuario utilizadas por los administradores del área de Transformación Digital y ciberseguridad
Objetivo	Si aplica

Ítem	Bien/Servicio	Datos, Descripción o Especificaciones Técnicas del Bien o Servicio	Cantidad	Unidad de Medida
1	BIEN	***Dispositivos de Autenticación Multifactor (MFA): YubiKey u otros compatibles FIDO2*** • Estándar de autenticación: **FIDO2/WebAuthn, U2F** • Soporte para USB-A, USB-C y/o NFC • Compatibilidad con sistemas operativos Windows, Linux, macOS, Android e iOS • Capacidad de almacenamiento seguro de claves criptográficas • Certificaciones de seguridad como Common Criteria EAL4+ o superior • Garantía mínima de 2 años	6	UN

Nota 1: Las columnas donde no aplique favor colocar N/A (No deben quedar espacios en blanco).

Nota 2: En caso de los bienes, si el mismo necesita garantía o muestra se debe especificar (si aplica).

Nota 3: En caso de los servicios, el solicitante debe describir las especificaciones que requiere; Experiencia/credenciales, calificaciones y competencias del personal que realizará el servicio, experiencia especifica, plan de trabajo, cronograma, Metodología y enfoque, personal mínimo requerido y tiempo de ejecución.

Agregar Imagen (Si aplica)

Disclaimer: las imágenes mostradas son solo para fines ilustrativos y pueden no ser la representación exacta del producto

ELABORADO POR:	APROBADO POR: (Director del área)

Solicitud No.			TIC-INT-69-25
Fecha:	04	07	2025

Nombre del Bien/Servicio	***Servidor para Laboratorio de Ciberdefensa y Virtualización***
Descripción y Uso	El objetivo de esta adquisición es generar herramientas de seguridad para crear: o Un entorno de simulación de redes corporativas reales o Prácticas de respuesta ante incidentes o Despliegue de entornos de ataque y defensa (red team / blue team) o Virtualización de herramientas de análisis, laboratorios de hacking ético y máquinas de
Objetivo	Si aplica

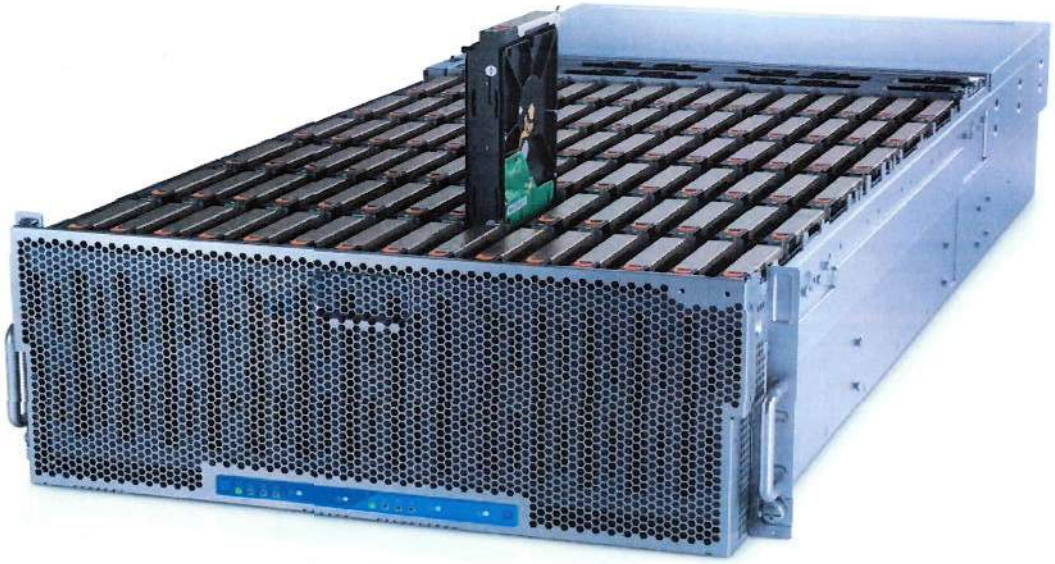
Ítem	Bien/Servicio	Datos, Descripción o Especificaciones Técnicas del Bien o Servicio	Cantidad	Unidad de Medida
2	BIEN	***Servidor para Laboratorio de Ciberdefensa y Virtualización:*** • **Especificaciones mínimas del servidor:** o Procesador: Intel Xeon o AMD EPYC, mínimo 8 núcleos (con soporte para virtualización VT-x/AMD-V) o Memoria RAM: **64 GB DDR4 ECC** o Almacenamiento: **2 TB SSD NVMe + 4 TB HDD** (*RAID* configurable) o Tarjetas de red: Doble puerto Gigabit Ethernet o Plataforma de virtualización: **VMware ESXi, Microsoft Hyper-V o Proxmox VE instalado** o Sistema operativo: CentOS/Ubuntu Server LTS o Windows Server 2022 o Conectividad remota segura (iLO, IPMI) o Garantía mínima: **3 años**	1	UN

Nota 1: Las columnas donde no aplique favor colocar N/A (No deben quedar espacios en blanco).

Nota 2: En caso de los bienes, si el mismo necesita garantía o muestra se debe especificar (si aplica).

Ítem	Bien/Servicio	Datos, Descripción o Especificaciones Técnicas del Bien o Servicio	Cantidad	Unidad de Medida
Nota 3: En caso de los servicios, el solicitante debe describir las especificaciones que requiere; Experiencia/credenciales, calificaciones y competencias del personal que realizará el servicio, experiencia especifica, plan de trabajo, cronograma, Metodología y enfoque, personal mínimo requerido y tiempo de ejecución.				

Agregar Imagen (Si aplica)



Disclaimer: las imágenes mostradas son solo para fines ilustrativos y pueden no ser la representación exacta del producto

ELABORADO POR:	APROBADO POR: *(Director del área)*

Solicitud No.	TIC-INT-69-25		
Fecha:	04	07	2025

Nombre del Bien/Servicio	Forti SIEM 2200G
Descripción y Uso	Es un dispositivo para la administración y monitoreo de eventos de seguridad de la red local de la institución
Objetivo	Si aplica

Ítem	Bien/Servicio	Datos, Descripción o Especificaciones Técnicas del Bien o Servicio	Cantidad	Unidad de Medida
3	Servicio	Forti SIEM 2200G • Capacidad de procesamiento de logs: mínimo **500 eventos por segundo (EPS)** o superior • *Almacenamiento local: SSD NVMe de alta capacidad para* indexado rápido • Interfaz de red: múltiples interfaces Gigabit Ethernet para segmentación de tráfico • Integración nativa con FortiGate 60F y otros dispositivos de red y seguridad • Licencia completa por **1 año,** renovable • *Garantía mínima:* ***3 años*** • Requerimientos de hardware/software según especificaciones oficiales de Fortinet • **Funcionalidades principales:** • Monitoreo centralizado de eventos de seguridad • Correlación de logs y detección avanzada de amenazas • Dashboard intuitivo con alertas en tiempo real • Informes de cumplimiento y análisis forense • Roles de usuario y auditoría de actividades	1	UN

Nota 1: Las columnas donde no aplique favor colocar N/A (No deben quedar espacios en blanco).

Nota 2: En caso de los bienes, si el mismo necesita garantía o muestra se debe especificar (si aplica).

Nota 3: En caso de los servicios, el solicitante debe describir las especificaciones que requiere; Experiencia/credenciales, calificaciones y competencias del personal que realizará el servicio, experiencia especifica, plan de trabajo, cronograma, Metodología y enfoque, personal mínimo requerido y tiempo de ejecución.

Agregar Imagen (Si aplica)

ELABORADO POR:	APROBADO POR: (Director del área)

Solicitud No.			TIC-INT-69-25
Fecha:	04	07	2025

Nombre del Bien/Servicio	**Capacitación Certificada para personal de Transformación digital y Ciberseguridad**
Descripción y Uso	Se incluye una formación técnica integral dirigida al personal responsable del manejo y mantenimiento de los equipos y servicios contratados
Objetivo	Si aplica

Ítem	Bien/Servicio	Datos, Descripción o Especificaciones Técnicas del Bien o Servicio	Cantidad	Unidad de Medida
4	Servicio	***Capacitación Certificada para personal de Transformación digital y Ciberseguridad*** • **CompTIA Network+**: Fundamentos de redes, diseño, configuración y solución de problemas. • **CompTIA Server+**: Administración y gestión de servidores físicos y virtuales. • **CompTIA Security+**: Fundamentos de seguridad informática, amenazas, vulnerabilidades, controles y cumplimiento. • Duración mínima: **40 horas presenciales o virtuales por certificación** • Incluye material oficial, laboratorios prácticos y preparación para exámenes oficiales.	5	UN

Nota 1: Las columnas donde no aplique favor colocar N/A (No deben quedar espacios en blanco).

Nota 2: En caso de los bienes, si el mismo necesita garantía o muestra se debe especificar (si aplica).

Nota 3: En caso de los servicios, el solicitante debe describir las especificaciones que requiere; Experiencia/credenciales, calificaciones y competencias del personal que realizará el servicio, experiencia especifica, plan de trabajo, cronograma, Metodología y enfoque, personal mínimo requerido y tiempo de ejecución.

Agregar Imagen (Si aplica)

ELABORADO POR:	APROBADO POR: (Director del área)

Solicitud No.			TIC-INT-69-25
Fecha:	04	07	2025

Nombre del Bien/Servicio	*Switches Cisco Catalyst Layer 3*
Descripción y Uso	Estos equipos permitirán establecer una red segura, escalable y altamente disponible, con capacidades integradas de detección de amenazas, control de acceso y visibilidad en tiempo real del estado de la infraestructura.
Objetivo	Si aplica

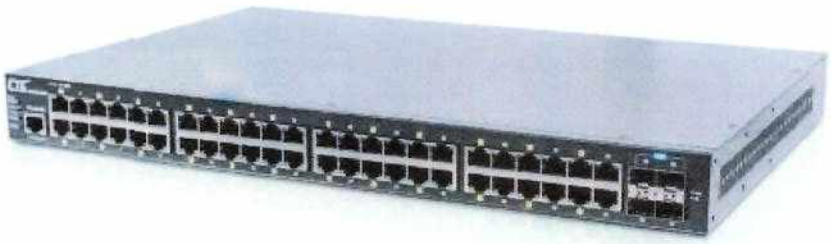
Ítem	Bien/Servicio	Datos, Descripción o Especificaciones Técnicas del Bien o Servicio	Cantidad	Unidad de Medida
5	Bienes/Servicios	**Switches Cisco Catalyst Layer 3** • Puertos: mínimo **24 puertos Gigabit Ethernet** • Interfaces SFP para uplink • Soporte para VLANs, QoS, STP, LACP • Gestión remota vía SNMPv3, SSH, HTTPS • Compatibilidad con IPv6 • Protocolos de seguridad: ACLs, Port Security, DHCP Snooping • Garantía mínima: **1 año**	15	UN

Nota 1: Las columnas donde no aplique favor colocar N/A (No deben quedar espacios en blanco).

Nota 2: En caso de los bienes, si el mismo necesita garantía o muestra se debe especificar (si aplica).

Nota 3: En caso de los servicios, el solicitante debe describir las especificaciones que requiere; Experiencia/credenciales, calificaciones y *competencias del personal que realizará el servicio, experiencia especifica, plan de trabajo, cronograma, Metodología y enfoque,* personal mínimo requerido y tiempo de ejecución.

Agregar Imagen (Si aplica)

Agregar Imagen (Si aplica)


Disclaimer: las imágenes mostradas son solo para fines ilustrativos y pueden no ser la representación exacta del producto

ELABORADO POR:	APROBADO POR: (Director del área)

Solicitud No.			TIC-INT-69-25
Fecha:	04	07	2025

Nombre del Bien/Servicio	**Herramientas fisicas de Pentesting**
Descripción y Uso	Dotar a la institución de herramientas físicas y entornos de simulación para análisis de ciberamenazas y respuesta ante incidentes.
Objetivo	Si aplica

Ítem	Bien/Servicio	Datos, Descripción o Especificaciones Técnicas del Bien o Servicio	Cantidad	Unidad de Medida
6	Bien/servicios	Herramientas físicas de Pentesting o Dispositivos portátiles tipo "Pineapple", "WiFi Pineapple Mark VII" o similar o Escáneres de vulnerabilidades inalámbricas o Sniffers de red físicos (E.G., SharkJack, LAN Turtle)	1	UN

Nota 1: Las columnas donde no aplique favor colocar N/A (No deben quedar espacios en blanco).

Nota 2: En caso de los bienes, si el mismo necesita garantía o muestra se debe especificar (si aplica).

Nota 3: En caso de los servicios, el solicitante debe describir las especificaciones que requiere; Experiencia/credenciales, calificaciones y competencias del personal que realizará el servicio, experiencia especifica, plan de trabajo, cronograma, Metodología y enfoque, personal mínimo requerido y tiempo de ejecución.

Agregar Imagen (Si aplica)

ELABORADO POR:	APROBADO POR: (Director del área)

INTRANT INSTITUTO NACIONAL DEL TRANSITO Y TRANSPORTE TERRESTRE Dirección de Tecnología de la Información

Solicitud No.			TIC-INT-69-25
Fecha:	04	07	2025

Nombre del Bien/Servicio	**Herramientas fisicas de Análisis Forense**
Descripción y Uso	Dotar a la institución de herramientas físicas y entornos de simulación para análisis de ciberamenazas y respuesta ante incidentes.
Objetivo	Si aplica

Ítem	Bien/Servicio	Datos, Descripción o Especificaciones Técnicas del Bien o Servicio	Cantidad	Unidad de Medida
7	Bienes/Servicios	**Herramientas físicas de Análisis Forense** o Estaciones de forense digital para extracción de datos o Dispositivos de bloqueo de escritura (write-blockers) o Kits de recolección de evidencia física o Lectores de memoria RAM volátil	1	UN

Nota 1: Las columnas donde no aplique favor colocar N/A (No deben quedar espacios en blanco).

Nota 2: En caso de los bienes, si el mismo necesita garantía o muestra se debe especificar (si aplica).

Nota 3: En caso de los servicios, el solicitante debe describir las especificaciones que requiere; Experiencia/credenciales, calificaciones y competencias del personal que realizará el servicio, experiencia especifica, plan de trabajo, cronograma, Metodología y enfoque, personal mínimo requerido y tiempo de ejecución.

Agregar Imagen (Si aplica)

ELABORADO POR:	APROBADO POR: (Director del área)

INTRANT
INSTITUTO NACIONAL DEL TRANSITO Y TRANSPORTE TERRESTRE
Dirección de Tecnología de la Información

Solicitud No.			TIC-INT-69-25
Fecha:	04	07	2025

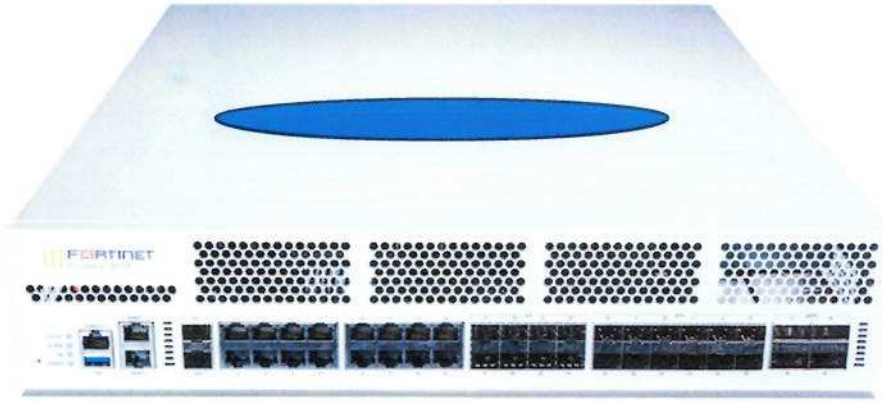
Nombre del Bien/Servicio	***Firewall FortiGate 60F y licencias***
Descripción y Uso	Implementar una infraestructura de telecomunicaciones segura, confiable y escalable en 5 sucursales
Objetivo	Si aplica

Ítem	Bien/Servicio	Datos, Descripción o Especificaciones Técnicas del Bien o Servicio	Cantidad	Unidad de Medida
8	***Bienes/servicios***	***Firewall FortiGate 60F y licenses*** • NGFW con protección avanzada contra amenazas • Soporte para VLANs, routing dinámico, IPS, filtrado web, cifrado SSL • Túneles IPsec y SSL VPN • Integración con FortiSIEM • Garantía mínima: **3 años** • Licenciamiento incluido	5	UN

Nota 1: Las columnas donde no aplique favor colocar N/A (No deben quedar espacios en blanco).

Nota 2: En caso de los bienes, si el mismo necesita garantía o muestra se debe especificar (si aplica).

Nota 3: En caso de los servicios, el solicitante debe describir las especificaciones que requiere; Experiencia/credenciales, calificaciones y competencias del personal que realizará el servicio, experiencia especifica, plan de trabajo, cronograma, Metodología y enfoque, personal mínimo requerido y tiempo de ejecución.

Agregar Imagen (Si aplica)

Disclaimer: las imágenes mostradas son solo para fines ilustrativos y pueden no ser la representación exacta del producto

ELABORADO POR:	APROBADO POR: (Director del área)

INTRANT
INSTITUTO NACIONAL DE TRÁNSITO
Y TRANSPORTE TERRESTRE

ESPECIFICACIONES TÉCNICAS

Adquisición de Bienes y servicios para el reforzamiento de la Ciberseguridad de la red institucional

1. DESCRIPCIÓN GENERAL DEL PROYECTO

La presente licitación tiene como finalidad fortalecer de manera integral la infraestructura tecnológica, de telecomunicaciones y la postura de ciberseguridad de INTRANT, con el objetivo de mejorar su capacidad operativa, garantizar la protección de la información sensible y asegurar la continuidad del negocio frente a amenazas cibernéticas cada vez más sofisticadas.

El proyecto se estructura en dos grandes componentes:

1.1 Fortalecimiento de la Ciberseguridad Institucional

Se busca adquirir herramientas físicas especializadas para análisis forense digital, pruebas de penetración (pen testing), autenticación multifactor (MFA) y un servidor con capacidad de virtualización para laboratorios de simulación de incidentes. Este componente permitirá dotar a la institución de capacidades avanzadas de defensa activa, detección de amenazas y respuesta ante incidentes de seguridad.

Además, se incluye la entrega de capacitación técnica certificada bajo estándares internacionales, enfocada en las certificaciones **CompTIA Security+, CompTIA CySA+** y **Fortinet NSE Series**, orientadas al personal técnico encargado de la gestión de la seguridad informática.

1.2 Modernización de la Infraestructura de Telecomunicaciones

Este componente tiene como propósito actualizar la infraestructura de red y seguridad en **10 sucursales** de la institución mediante la adquisición e instalación de equipos de telecomunicaciones estratégicos, incluyendo:

- **Firewall FortiGate 60F** en cada sede
- **Switches Cisco Catalyst Layer 3**
- **Sistema automatizado de protección, detección y respuesta (EDR)**

Estos equipos permitirán establecer una red segura, escalable y altamente disponible, con capacidades integradas de detección de amenazas, control de acceso y visibilidad en tiempo real del estado de la *infraestructura*.

1.3 Capacitación Técnica Certificada

Como parte fundamental del proyecto, se incluye una formación técnica integral dirigida al personal responsable del manejo y mantenimiento de los equipos y servicios contratados. La capacitación cubrirá las siguientes certificaciones reconocidas internacionalmente:

- **CompTIA Network+**: Enfocada en fundamentos de redes, diseño, configuración y solución de problemas.
- **CompTIA Server+**: Orientada a la administración y gestión de servidores físicos y virtuales.
- **Fortinet NSE Series**: Especialización en gestión de firewalls, monitoreo de eventos de seguridad y protección contra amenazas avanzadas.

La duración total de la capacitación será de **mínimo 80 horas**, combinando teoría, laboratorios prácticos y preparación para exámenes oficiales si aplica.

2. OBJETIVO GENERAL

El objetivo principal del proyecto es modernizar y reforzar la infraestructura tecnológica y de ciberseguridad de la institución, mejorando su resiliencia frente a amenazas digitales, optimizando la conectividad entre sucursales y asegurando la protección de los datos sensibles bajo su custodia.

3. METAS DEL PROYECTO

- Implementar una infraestructura de telecomunicaciones segura, confiable y escalable en 5 sucursales.
- Dotar a la institución de herramientas físicas y entornos de simulación para análisis de ciberamenazas y respuesta ante incidentes.
- Capacitar al personal técnico en competencias certificadas en redes, servidores y ciberseguridad.
- Establecer un Sistema automatizado de protección, detección y respuesta (EDR).
- Promover la autonomía técnica y operativa del equipo interno mediante formación especializada.

4. FORMA DE PAGO

El pago se realizará en **tres cuotas:**

1. **Primera cuota (30%):** Al inicio del contrato, previa recepción de los documentos contractuales.
2. **Segunda cuota (30%):** Después de la entrega física de los equipos y configuración inicial.
3. **Tercera cuota (40%):** Una vez finalizada la capacitación técnica y validados todos los servicios contratados.

5. ALCANCE

El alcance del contrato incluye:

- **Servicios de ciberseguridad:** capacitación certificada.
- **Equipos de telecomunicaciones y Seguridad:** Firewalls de próxima generación, switches Cisco Catalyst Layer 2 y 3, servidor de virtualización, Sistema automatizado de protección, detección y respuesta (EDR).
- **Capacitación técnica:** CompTIA Network+, CompTIA Server+, CompTIA Security+, Fortinet NSE series.

6. TIEMPO DE ENTREGA

- Máximo **90 días calendario** desde la firma del contrato, incluyendo:
  - Entrega de equipos
  - Configuración inicial
  - Capacitación técnica
  - Pruebas finales

7. TIEMPO DE LOS BIENES Y SERVICIOS

Los bienes y servicios contratados tendrán una vigencia mínima de **1 año**, con soporte técnico postventa durante todo este período.

8. BIENES Y SERVICIOS A ADQUIRIRSE Y SUS ESPECIFICACIONES

a) Herramientas Físicas de Ciberseguridad

i) Dispositivos de Autenticación Multifactor (MFA):

- **Cantidad requerida:** 6 unidades
- **Estándar de autenticación:** FIDO2/WebAuthn, U2F
- **Soporte:** USB-A, USB-type C y/o NFC
- **Compatibilidad:** Windows, Linux, macOS, Android, iOS
- **Certificaciones de seguridad:** Common Criteria EAL4+ o superior
- **Garantía mínima:** 2 años

ii) Herramientas Físicas de Pen Testing y Análisis Forense

- **Penetration Testing:**
  - Dispositivos portátiles tipo "Pineapple", "WiFi Pineapple Mark VII" o similar
  - Escáneres de vulnerabilidades inalámbricas
  - Sniffers de red físicos (E.G., SharkJack, LAN Turtle)
- **Análisis Forense:**
  - Estaciones de forense digital para extracción de datos
  - Dispositivos de bloqueo de escritura (write-blockers)
  - Kits de recolección de evidencia física
  - Lectores de memoria RAM volátil

b) Equipo de Virtualización y Laboratorio de Ciberdefensa

- **Servidor:**
  - Procesador: Intel Xeon o AMD EPYC, mínimo 8 núcleos
  - Memoria RAM: **64 GB DDR4 ECC**
  - Almacenamiento: **2 TB SSD NVMe + 4 TB HDD**
  - Plataforma de virtualización: VMware ESXi, Microsoft Hyper-V o Proxmox VE
  - Sistema operativo: CentOS/Ubuntu Server LTS o Windows Server 2022
  - Garantía mínima: **3 años**

c) Equipos de Telecomunicaciones

i) Firewall de próxima generación – 5 Unidades

- NGFW con protección avanzada contra amenazas
- Soporte para VLANs, routing dinámico, IPS, filtrado web, cifrado SSL
- Túneles IPsec y SSL VPN
- Integración con FortiSIEM,FortiManager y FortiAnalyser
- Garantía mínima: **3 años**
- Licenciamiento incluido

ii) Sistema automatizado de protección, detección y respuesta (EDR) – *1 Unidad*

- Protección Integral de Endpoints.
- Detección y respuesta en tiempo real en endpoints físicos y virtuales (Windows, macOS, Linux).
- Prevención de ejecución de malware y ransomware sin depender únicamente de firmas.
- Gestión Centralizada y Automatización
- Consola de administración única para monitoreo y respuesta.
- Alertas inteligentes y automatización de acciones (aislamiento de equipos, eliminación de amenazas, etc.).
- Informes de cumplimiento y análisis forense.
- Análisis de comportamiento y detección de anomalías.
  Gestión Centralizada y Automatización.

iii) Switches Cisco Catalyst Layer 3– *15 Unidades*

- Puertos: mínimo **24 puertos Gigabit Ethernet**
- Interfaces SFP para uplink
- Soporte para VLANs, QoS, STP, LACP
- Gestión remota vía SNMPv3, SSH, HTTPS

- Compatibilidad con IPv6
- Protocolos de seguridad: ACLs, Port Security, DHCP Snooping
- Garantía mínima: **1 año**
- Compatible con Switches Cisco y productos fortinet

9. REQUERIMIENTOS ESPECÍFICOS

a) Capacitación Certificada

- **CompTIA Network+**: Fundamentos de redes, diseño, configuración y solución de problemas.
- **CompTIA Server+**: Administración y gestión de servidores físicos y virtuales.
- **CompTIA Security+**: Fundamentos de seguridad informática, amenazas, vulnerabilidades, controles y cumplimiento.
- Duración mínima: **40 horas presenciales o virtuales por certificación**
- Incluye material oficial, laboratorios prácticos y preparación para exámenes oficiales.

b) Requerimientos de Seguridad

- Cumplimiento con la **Ley 133-17 sobre Protección de Datos Personales**.
- Implementación de políticas de seguridad basadas en estándares internacionales (ISO 27001, NIST).

10. REQUERIMIENTOS GENERALES

El proveedor deberá:

- Ser empresa legalmente constituida en República Dominicana o contar con representante autorizado.
- Tener experiencia demostrable en proyectos similares (mínimo 3 proyectos en los últimos 5 años).
- Contar con personal técnico certificado en ciberseguridad, redes y sistemas.
- Brindar soporte técnico postventa por al menos **1 año**.
- Proporcionar documentación técnica oficial de los equipos y software ofrecidos.

11. CONDICIONES GENERALES

- El contrato se regirá bajo lo establecido en la **Ley General de Contratación Pública No. 340-06**.
- Los equipos deben ser nuevos, sellados y con garantía mínima de **1 año**.
- La capacitación técnica será impartida en idioma español.
- Se exigirá cumplimiento con normativas locales e internacionales aplicables.

12. CRITERIOS DE CONDICIONES DE PAGO

- Pago en tres cuotas según el plan detallado en la sección **Forma de Pago**.
- Revisión y aprobación de facturas antes de cada pago.

13. FACTURACIÓN Y CONDICIONES DE ENTREGA

- Facturación detallada por ítem, incluyendo:
  - Equipos adquiridos
  - Servicios prestados
  - Capacitación certificada
- Entrega física de todos los equipos en las sucursales designadas.
- Acta de recepción firmada por ambas partes.

El presente documento de especificaciones técnicas ha sido elaborado por el equipo técnico del INTRANT el 25 de marzo de 2025.

14. CAPÍTULO: ENTREGA, INSTALACIÓN Y PUESTA EN MARCHA DE LOS EQUIPOS

1. OBJETIVO DEL CAPÍTULO

El presente capítulo tiene como finalidad establecer los requisitos técnicos y operativos relacionados con la **entrega física, instalación e implementación de los equipos adquiridos**, asegurando que cada dispositivo quede completamente configurado, probado y listo para su uso inmediato por parte del personal técnico autorizado.

2. DESCRIPCIÓN GENERAL

Todos los equipos adquiridos dentro del marco de esta licitación deberán ser entregados **instalados, configurados y funcionando correctamente** en las ubicaciones definidas (10 sucursales), según lo acordado en el contrato. El proveedor será responsable de garantizar la correcta integración de los dispositivos en la infraestructura existente y su operación inmediata desde el momento de la recepción.

3. REQUISITOS GENERALES DE ENTREGA E INSTALACIÓN

a) Entrega Física

- Todos los equipos deben ser nuevos, sellados, con número de serie visible y cumpliendo con los estándares de fábrica.
- Se deberá entregar documentación técnica oficial del fabricante, manuales de usuario, drivers, firmware actualizado y licencias correspondientes.

b) Instalación en Sitio

- El proveedor deberá coordinar e implementar la instalación de todos los equipos en las **10 sucursales designadas**.
- La instalación incluye:
  - Desempaque y verificación física
  - Montaje físico en racks o espacios asignados
  - Conexión eléctrica y de red seguras y organizadas
  - Configuración inicial de acceso y conectividad básica

c) Configuración Inicial

- Cada equipo deberá ser configurado conforme a los parámetros técnicos definidos por la institución o, en su defecto, siguiendo buenas prácticas de seguridad y estándares reconocidos (ej.: CIS Benchmarks).
- La configuración mínima incluirá:
  - Asignación de direcciones IP
  - Configuración de interfaces y VLANs
  - Establecimiento de políticas básicas de seguridad
  - Integración con sistemas de monitoreo existentes (FortiSIEM, SIEM, etc.)
  - Configuración de usuarios administradores y roles de acceso

d) Pruebas Funcionales

- Una vez instalado y configurado, cada equipo deberá pasar pruebas funcionales que demuestren su operatividad:
  - Comunicación de red exitosa
  - Aplicación correcta de reglas de firewall y control de acceso
  - Registro de logs y monitoreo de dispositivos (donde aplique)
  - Pruebas de conectividad y rendimiento
- Estas pruebas deberán ser validadas y firmadas por representantes de la institución.

e) Acta de Recepción Técnica

- Por cada sede o grupo de equipos instalados, se deberá generar un **acta de recepción técnica**, firmada por el proveedor y el responsable de la institución.
- El acta deberá incluir:
  - Detalle del equipo instalado (modelo, serial, ubicación)
  - Resultados de las pruebas realizadas
  - Confirmación de operación correcta
  - Observaciones y recomendaciones técnicas

4. UBICACIONES DE INSTALACIÓN

Las ubicaciones serán proporcionadas al adjudicatario antes del inicio de las actividades.

5. DOCUMENTACIÓN DE SOPORTE

Como parte del proceso de instalación, el proveedor deberá entregar al término de cada actividad:

- Manual de usuario del equipo
- Guía de configuración realizada
- Diagramas de red actualizados (si aplica)
- Copias de las configuraciones aplicadas
- Contraseñas de acceso iniciales (en sobre sellado, bajo protocolo de seguridad)

6. GARANTÍA POST-INSTALACIÓN

El proveedor deberá garantizar la operación correcta de los equipos durante un periodo mínimo de **30 días posteriores a la firma del acta de recepción**. Durante este tiempo, cualquier ajuste necesario derivado de la puesta en marcha será responsabilidad del proveedor sin costo adicional.

7. CRITERIOS DE ACEPTACIÓN FINAL

Para considerar completada la entrega e instalación de los equipos, se deberán cumplir los siguientes criterios:

- Equipos físicamente instalados en las ubicaciones definidas
- Totalmente configurados y operativos
- Documentación técnica completa y actualizada

- Acta de recepción firmada por ambas partes
- Capacitación realizada (según cronograma establecido)

8. RESPONSABILIDADES DEL PROVEEDOR

- Proporcionar personal técnico certificado para la instalación y configuración de los equipos
- Garantizar compatibilidad con la infraestructura actual
- Coordinar logística y transporte seguro de los equipos a cada sucursal
- Realizar reporte técnico por cada sitio visitado
- Asegurar que el proceso no genere interrupciones significativas en los servicios operativos

9. RESPONSABILIDADES DE LA INSTITUCIÓN

- Proveer acceso físico a los sitios de instalación
- Designar personal técnico responsable de acompañar la instalación
- Facilitar información relevante de la infraestructura existente (redes, IPs, VLANs, etc.)

10. CONSIDERACIONES ADICIONALES

- No se aceptará la entrega de equipos sin haber sido previamente instalados y verificados.
- En caso de fallas técnicas detectadas durante la puesta en marcha, el proveedor deberá corregirlas o sustituir los equipos en un plazo máximo de **5 días hábiles**.
- La institución se reserva el derecho de inspeccionar y validar la calidad del trabajo realizado en cualquiera de las sucursales.

EUDIS ORTIZ LEDESMA
Departamento de Ciberseguridad

INTRANT
INSTITUTO NACIONAL DE TRÁNSITO Y TRANSPORTE TERRESTRE
Dirección de Tecnología de la Información

MICHAEL ORTIZ
ADMINISTRADOR DE REDES

---Fin del Documento--

INTRANT
INSTITUTO NACIONAL DE TRÁNSITO
Y TRANSPORTE TERRESTRE

INFORME JUSTIFICATIVO DE ESPECIFICACION DE MARCA

1. Introducción

El presente informe tiene como objetivo justificar la solicitud de especificación de marca en la adquisición de los siguientes bienes:

- **Switches Cisco Catalyst Layer 3**
- **Firewall FortiGate 60F**

Dicha excepción se fundamenta en la necesidad de mantener la coherencia, interoperabilidad, estabilidad y seguridad de la infraestructura de red institucional, la cual ha sido diseñada, implementada y operacionalizada bajo plataformas tecnológicas específicas que garantizan el cumplimiento de estándares de rendimiento, confiabilidad y gestión centralizada.

La adquisición de estos equipos no se realiza por preferencia comercial, sino por imperativos técnicos derivados de la arquitectura actual de la red interna, que requiere soluciones integradas, homogéneas y certificadas para asegurar el funcionamiento óptimo de servicios críticos.

2. Switches Cisco Catalyst Layer 3

La infraestructura de red interna de la institución se encuentra actualmente estructurada sobre dispositivos de marca **Cisco**, específicamente switches **Catalyst Layer 3**, que son componentes clave en la arquitectura de red de núcleo y distribución.

Estos dispositivos son **switches gestionables de alto rendimiento**, diseñados para redes empresariales que requieren capacidades avanzadas de **conmutación (capa 2)** y **enrutamiento IP (capa 3)** dentro de una misma plataforma. Su uso permite:

- Segmentación inteligente del tráfico mediante VLANs.
- Enrutamiento entre subredes sin necesidad de routers externos.
- Aplicación de políticas de **Calidad de Servicio (QoS)** y **seguridad**.
- Alta disponibilidad y redundancia mediante protocolos como VRRP, HSRP y STP.
- Integración con herramientas de monitoreo y gestión de red (como Cisco DNA Center, SNMP, etc.).

La inclusión de nuevos switches de otras marcas generaría incompatibilidades en:

- Protocolos de enrutamiento dinámico (OSPF, EIGRP).
- Configuraciones de VLAN y troncales (802.1Q).
- Interfaz de administración y gestión remota.
- Soporte técnico especializado y actualizaciones de firmware

Firewall FortiGate 60F con Licencias de Seguridad

La plataforma de seguridad perimetral de la institución está basada íntegramente en tecnología **Fortinet,** siendo el **FortiGate 60F** el dispositivo principal que protege la red contra amenazas cibernéticas. Esta solución forma parte de una **infraestructura homogénea de seguridad** que incluye:

- **FortiManager:** para gestión centralizada de políticas, configuraciones y actualizaciones.
- **FortiAnalyzer:** para análisis de logs, auditorías y detección de comportamientos anómalos.
- **FortiClient:** para acceso seguro remoto y endpoint protection.

El **FortiGate 60F** es un **firewall de próxima generación (NGFW)** que ofrece funciones críticas como:

- Filtrado de contenido y aplicaciones.
- Prevención de intrusiones (IPS).
- Antivirus, antimalware y sandboxing.
- VPN IPSec/SSL para acceso remoto seguro.
- Control de ancho de banda y QoS.
- Inspección profunda de paquetes (DPI).

La integración de este dispositivo con las licencias de seguridad garantiza:

- **Actualizaciones automáticas** de firmas de malware y reglas de seguridad.
- **Gestión unificada** desde herramientas centrales.
- **Reducción de complejidad operativa** al evitar múltiples sistemas de seguridad heterogéneos.
- **Soporte técnico especializado** certificado por Fortinet.
- **Escalabilidad futura** hacia modelos más robustos dentro de la misma familia de productos.

La sustitución de este equipo por uno de otra marca implicaría:

- Pérdida de compatibilidad con el ecosistema Fortinet.
- Dificultades en la migración de políticas de seguridad.
- Incremento del riesgo de brechas de seguridad por mal configuración.
- Mayor costo operativo debido a la necesidad de capacitación en nuevas tecnologías.

Fundamentos Legales y Normativos

La excepción solicitada se ajusta a los lineamientos establecidos en normativas nacionales de contratación pública, tales como:

- **Ley de Contrataciones del Estado** (artículo 47, inciso b): Permite la adquisición directa cuando existe **exclusividad técnica** o **incompatibilidad con otros productos.**
- **Reglamento de la Ley de Contrataciones del Estado**: Se considera justificada la exclusividad cuando el bien o servicio no puede ser sustituido por otros equivalentes sin afectar el funcionamiento del sistema existente.
- **Directrices de interoperabilidad y estandarización tecnológica**: La institución ha adoptado una política de estandarización de plataformas para reducir costos, mejorar soporte y fortalecer la seguridad.

Distribuidores autorizados de Fortinet

Nombre Comercial	RNC
MetricTouch SRL – Distribuidor autorizado que ofrece equipos, licencias, hardware, consultoría y entrenamientos Fortinet en Santo Domingo.	1-31-20053-5
Multicómputos – MSP e integrador con más de 20 años en el mercado dominicano, con Fortinet en su portafolio.	1-31-07021-0
TCO Networks – Empresa que brinda soluciones de cloud, almacenamiento, firewall y Fortinet.	1-31-17298-8
Wesolve Technologies – Proveedor de soluciones de endpoint security, firewall y Fortinet, entre otras tecnologías.	1-31-18559-3
Justech – Especializados en servicios como virtualización, respaldo y seguridad (incluyendo Fortinet).	1-31-16688-7

Imnovaty – Ofrece Fortinet junto a soluciones ERP, backup, email y VOIP.	1-31-16448-5
Infomatic SRL – Reseller de virtualización, backup, firewall y seguridad; Fortinet está en su oferta.	4-31-10513-4
SJVR – Consultores en Microsoft, firewall y seguridad; incluyen Fortinet entre sus productos.	4-31-12388-0
Solutek B2B – Especializados en venta y cotización de firewalls Fortinet en Santo Domingo, con asesoría técnica.	4-31-13678-2
Ingeniería y Sistemas S.A. (Ingesis)	1-01-76493-3
Telsys S.A.	1-31-06549-8
Data Systems S.A.	1-31-00967-0
Netcore S.A.	

Distribuidores autorizados de Cisco

Ingeniería y Sistemas S.A. (Ingesis) – Partner Gold de Cisco, distribuye y soporta switches Catalyst, routers, firewalls y soluciones de red.	1-01-76493-3
Telsys S.A. – Partner Silver de Cisco, ofrece equipos de red, seguridad y colaboración.	1-31-06549-8
Data Systems S.A. – Partner registrado de Cisco, provee infraestructura de red para sector público.	1-31-00967-0
Netcore S.A. – Revendedor autorizado, especializado en redes Cisco (Catalyst, ISR).	1-31-15211-8
CompuGroup S.A. – Ofrece soluciones Cisco en redes y comunicaciones unificadas.	1-31-00211-8
Claro República Dominicana – Integra soluciones Cisco en proyectos de red empresarial y gubernamental.	1-31-01783-7
Altice Dominicana – Utiliza y ofrece tecnologías Cisco en soluciones de conectividad y seguridad.	1-31-04152-8

Conclusión

La adquisición de los **Switches Cisco Catalyst Layer 3** y el **Firewall FortiGate 60F con licencias** no constituye una preferencia comercial, sino una **necesidad técnica imperiosa** para:

- Mantener la **integridad y coherencia** de la infraestructura de red.
- Garantizar la **interoperabilidad, gestión centralizada** y **escalabilidad**.
- Preservar la **seguridad institucional** frente a amenazas cibernéticas.
- Optimizar el uso del conocimiento técnico del personal.
- Evitar costos adicionales derivados de migraciones, capacitaciones y fallos de compatibilidad.

Por lo tanto, se solicita formalmente la **excepción por exclusividad técnica** para proceder con la adquisición directa de estos equipos, conforme a los principios de racionalidad, eficiencia y seguridad en la gestión de recursos tecnológicos.

ELABORADO POR:	**APROBADO POR:** **(Director del área)**

INTRANT
INSTITUTO NACIONAL DEL TRÁNSITO Y TRANSPORTE TERRESTRE
Dirección de Tecnología de la Información