	DIRECCIÓN ADMINISTRATIVO FINANCIERO	FO.GAF.02
		VERSIÓN 1.0
	FICHA TÉCNICA PARA ADQUISICIÓN DE BIENES Y SERVICIOS	FECHA DE REVISIÓN: 17 de marzo 2025

Solicitud No.	
Fecha:	

Nombre del Bien/Servicio	Dispositivos de Autenticación Multifactor (MFA):
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	<p>Dispositivos de Autenticación Multifactor (MFA):</p> <ul style="list-style-type: none"> 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


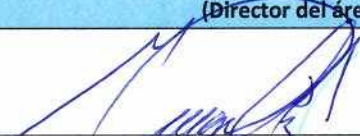
Nota 1: Las columnas donde no aplique favor colocar N/A (No deben quedar espacios en blanco).

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 específica, plan de trabajo, cronograma, Metodología y enfoque, personal mínimo requerido y tiempo de ejecución.

Agregar Imagen (Si aplica)

	DIRECCIÓN ADMINISTRATIVO FINANCIERO	FO.GAF.02
	FICHA TÉCNICA PARA ADQUISICIÓN DE BIENES Y SERVICIOS	VERSIÓN 1.0 FECHA DE REVISIÓN: 17 de marzo 2025

ELABORADO POR:	APROBADO POR: (Director del área)
	




 INTRANT <small>INSTITUTO NACIONAL DE TRANSITO Y TRANSPORTE TERRESTRE</small>	DIRECCIÓN ADMINISTRATIVO FINANCIERO	FO.GAF.02
		VERSIÓN 1.0
	FICHA TÉCNICA PARA ADQUISICIÓN DE BIENES Y SERVICIOS	FECHA DE REVISIÓN: 17 de marzo 2025

Solicitud No.	
Fecha:	

Nombre del Bien/Servicio	<i>Servidor para Laboratorio de Ciberdefensa y Virtualización</i>
Descripción y Uso	<p>El objetivo de esta adquisición es generar herramientas de seguridad para crear:</p> <ul style="list-style-type: none"> ○ Un entorno de simulación de redes corporativas reales ○ Prácticas de respuesta ante incidentes ○ Despliegue de entornos de ataque y defensa (red team / blue team) ○ 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	<i>Bien</i>	<p><i>Servidor para Laboratorio de Ciberdefensa y Virtualización</i></p> <ul style="list-style-type: none"> ● Especificaciones mínimas del servidor: <ul style="list-style-type: none"> ○ Procesador: Intel Xeon o AMD EPYC, mínimo 8 núcleos (con soporte para virtualización VT-x/AMD-V) ○ Memoria RAM: 64 GB DDR4 ECC ○ Almacenamiento: 2 TB SSD NVMe + 4 TB HDD (RAID configurable) ○ Tarjetas de red: Doble puerto Gigabit Ethernet ○ Plataforma de virtualización: VMware ESXi, Microsoft Hyper-V o Proxmox VE instalado ○ Sistema operativo: CentOS/Ubuntu Server LTS o Windows Server 2022 ○ Conectividad remota segura (iLO, IPMI) ○ Garantía mínima: 3 años 	1	UN

	DIRECCIÓN ADMINISTRATIVO FINANCIERO	FO.GAF.02
	FICHA TÉCNICA PARA ADQUISICIÓN DE BIENES Y SERVICIOS	VERSIÓN 1.0



Ítem	Bien/Servicio	Datos, Descripción o Especificaciones Técnicas del Bien o Servicio	Cantidad	Unidad de Medida

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 específica, 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 <small>INSTITUTO NACIONAL DE TRANSITO Y TRANSPORTE TERRESTRE</small>	DIRECCIÓN ADMINISTRATIVO FINANCIERO	FO.GAF.02
		VERSIÓN 1.0
	FICHA TÉCNICA PARA ADQUISICIÓN DE BIENES Y SERVICIOS	FECHA DE REVISIÓN: 17 de marzo 2025

Solicitud No.	TIC-INT-69-25
Fecha:	

Nombre del Bien/Servicio	Herramientas físicas 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	Bien	<ul style="list-style-type: none"> • Herramientas físicas de Análisis Forense <ul style="list-style-type: none"> ○ 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 	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 específica, plan de trabajo, cronograma, Metodología y enfoque, personal mínimo requerido y tiempo de ejecución.

Agregar Imagen (Si aplica)

	DIRECCIÓN ADMINISTRATIVO FINANCIERO	FO.GAF.02
	FICHA TÉCNICA PARA ADQUISICIÓN DE BIENES Y SERVICIOS	VERSIÓN 1.0 FECHA DE REVISIÓN: 17 de marzo 2025

ELABORADO POR:	APROBADO POR: (Director del área)
	



 INTRANT <small>INSTITUTO NACIONAL DE TRANSITO Y TRANSPORTE TERRESTRE</small>	DIRECCIÓN ADMINISTRATIVO FINANCIERO	FO.GAF.02
		VERSIÓN 1.0
	FICHA TÉCNICA PARA ADQUISICIÓN DE BIENES Y SERVICIOS	FECHA DE REVISIÓN: 17 de marzo 2025

Solicitud No.	
Fecha:	

Nombre del Bien/Servicio	Herramientas físicas de Pentesting
Descripción y Uso	<p>El objetivo de esta adquisición es generar herramientas de seguridad para crear:</p> <ul style="list-style-type: none"> ○ Un entorno de simulación de redes corporativas reales ○ Prácticas de respuesta ante incidentes ○ Despliegue de entornos de ataque y defensa (red team / blue team) ○ 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
6	Bien	Herramientas físicas de Pentesting <ul style="list-style-type: none"> ○ Dispositivos portátiles tipo "Pineapple", "WiFi Pineapple Mark VII" o similar ○ Escáneres de vulnerabilidades inalámbricas ○ 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 específica, plan de trabajo, cronograma, Metodología y enfoque, personal mínimo requerido y tiempo de ejecución.

Agregar Imagen (Si aplica)

	DIRECCIÓN ADMINISTRATIVO FINANCIERO	FO.GAF.02
	FICHA TÉCNICA PARA ADQUISICIÓN DE BIENES Y SERVICIOS	VERSIÓN 1.0

ELABORADO POR:	APROBADO POR: (Director del área)
	



 INTRANT <small>INSTITUTO NACIONAL DE TRANSITO Y TRANSPORTE TERRESTRE</small>	DIRECCIÓN ADMINISTRATIVO FINANCIERO	FO.GAF.02
		VERSIÓN 1.0
	FICHA TÉCNICA PARA ADQUISICIÓN DE BIENES Y SERVICIOS	FECHA DE REVISIÓN: 17 de marzo 2025

Solicitud No.	
Fecha:	

Nombre del Bien/Servicio	<i>Switches Cisco Catalyst Layer 3</i>
Descripción y Uso	<p>El objetivo de esta adquisición es generar herramientas de seguridad para crear:</p> <ul style="list-style-type: none"> ○ Un entorno de simulación de redes corporativas reales ○ Prácticas de respuesta ante incidentes ○ Despliegue de entornos de ataque y defensa (red team / blue team) ○ 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
5	Bien	<p>Switches Cisco Catalyst Layer 3</p> <ul style="list-style-type: none"> ● 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 <p>○</p>	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 específica, plan de trabajo, cronograma, Metodología y enfoque, personal mínimo requerido y tiempo de ejecución.

Agregar Imagen (Si aplica)

	DIRECCIÓN ADMINISTRATIVO FINANCIERO	FO.GAF.02
		VERSIÓN 1.0
	FICHA TÉCNICA PARA ADQUISICIÓN DE BIENES Y SERVICIOS	FECHA DE REVISIÓN: 17 de marzo 2025

ELABORADO POR:	APROBADO POR: (Director del área)
	



 INTRAN <small>INSTITUTO NACIONAL DE TRANSITO Y TRANSPORTE TERRESTRE</small>	DIRECCIÓN ADMINISTRATIVO FINANCIERO	FO.GAF.02
		VERSIÓN 1.0
	FICHA TÉCNICA PARA ADQUISICIÓN DE BIENES Y SERVICIOS	FECHA DE REVISIÓN: 17 de marzo 2025

Solicitud No.	
Fecha:	

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	<p>Capacitación Certificada para personal de Transformación digital y Ciberseguridad</p> <ul style="list-style-type: none"> • 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 específica, plan de trabajo, cronograma, Metodología y enfoque, personal mínimo requerido y tiempo de ejecución.

Agregar Imagen (Si aplica)

	DIRECCIÓN ADMINISTRATIVO FINANCIERO	FO.GAF.02
	FICHA TÉCNICA PARA ADQUISICIÓN DE BIENES Y SERVICIOS	VERSIÓN 1.0

ELABORADO POR:	APROBADO POR: (Director del área)
	



	DIRECCIÓN ADMINISTRATIVO FINANCIERO	FO.GAF.02
		VERSIÓN 1.0
	FICHA TÉCNICA PARA ADQUISICIÓN DE BIENES Y SERVICIOS	FECHA DE REVISIÓN: 17 de marzo 2025

Solicitud No.	TIC-INT-69-25
Fecha:	

Nombre del Bien/Servicio	<i>Firewall FortiGate 60F y licencias</i>
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	Bien	<ul style="list-style-type: none"> <i>Firewall FortiGate 60F y licencias</i> 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 específica, plan de trabajo, cronograma, Metodología y enfoque, personal mínimo requerido y tiempo de ejecución.

Agregar Imagen (Sí aplica)

	DIRECCIÓN ADMINISTRATIVO FINANCIERO	FO.GAF.02
		VERSIÓN 1.0
	FICHA TÉCNICA PARA ADQUISICIÓN DE BIENES Y SERVICIOS	FECHA DE REVISIÓN: 17 de marzo 2025

ELABORADO POR:	APROBADO POR: (Director del área)
	




 INTRANT <small>INSTITUTO NACIONAL DE TRANSITO Y TRANSPORTE TERRESTRE</small>	DIRECCIÓN ADMINISTRATIVO FINANCIERO	FO.GAF.02
	FICHA TÉCNICA PARA ADQUISICIÓN DE BIENES Y SERVICIOS	VERSIÓN 1.0
		FECHA DE REVISIÓN: 17 de marzo 2025

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

Nombre del Bien/Servicio	Sistema automatizado de protección, detección y respuesta (EDR)
Descripción y Uso	Es un dispositivo para proteger todos los activos digitales de una organización, desde el perímetro de red hasta los dispositivos finales, pasando por la nube, datos sensibles y usuarios.
Objetivo	

Ítem	Bien/Servicio	Datos, Descripción o Especificaciones Técnicas del Bien o Servicio	Cantidad	Unidad de Medida
3	Bien/servicio	<p>Protección Integral de Endpoints:</p> <ul style="list-style-type: none"> • 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. • Análisis de comportamiento y detección de anomalías. <p>Integración con Fortinet Security Fabric:</p> <ul style="list-style-type: none"> • Integración nativa con FortiGate, FortiSIEM, FortiSOAR y FortiXDR para una visión unificada de amenazas. • Correlación de eventos entre red, nube y endpoints. • Respuesta automatizada coordinada a nivel de red y endpoint. <p>Soporte de Autenticación Física: YubiKey:</p> <ul style="list-style-type: none"> • Compatibilidad con YubiKey 4, 5 y YubiKey Bio para: <ul style="list-style-type: none"> ○ Autenticación multifactor (MFA) en el acceso a la consola de administración de FortiEDR. ○ Acceso seguro a endpoints protegidos mediante credenciales FIDO2/WebAuthn. ○ Cifrado y firma digital para usuarios y administradores. • Integración con protocolos estándar como FIDO2, U2F, PIV, OpenPGP. 	1	UN

 INTRANT <small>INSTITUTO NACIONAL DE TRANSITO Y TRANSPORTE TERRESTRE</small>	DIRECCIÓN ADMINISTRATIVO FINANCIERO	FO.GAF.02
	FICHA TÉCNICA PARA ADQUISICIÓN DE BIENES Y SERVICIOS	VERSIÓN 1.0
		FECHA DE REVISIÓN: 17 de marzo 2025

Ítem	Bien/Servicio	Datos, Descripción o Especificaciones Técnicas del Bien o Servicio	Cantidad	Unidad de Medida
		<p>Despliegue Flexible:</p> <ul style="list-style-type: none"> • Opciones de despliegue: <ul style="list-style-type: none"> ○ SaaS (en la nube): Sin necesidad de hardware local. ○ On-premises: Con servidores dedicados para clientes que requieren control total del dato. • Compatible con entornos híbridos y multinube. <p>Gestión Centralizada y Automatización</p> <ul style="list-style-type: none"> • 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. <p>Requisitos de Hardware en Endpoints:</p> <ul style="list-style-type: none"> • Procesador: 1 GHz o superior • Memoria RAM: 2 GB mínimo (4 GB recomendado) • Disco: 1 GB de espacio libre • Red: Conexión activa a internet o red corporativa <p>Licenciamiento y soporte</p> <ul style="list-style-type: none"> • 3 años 		

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 específica, 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)**





ESPECIFICACIONES TÉCNICAS

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

1. DESCRIPCIÓN GENERAL DEL PROYECTO	4
1.1 Fortalecimiento de la Ciberseguridad Institucional.....	4
1.2 Modernización de la Infraestructura de Telecomunicaciones	4
1.3 Capacitación Técnica Certificada	4
2. OBJETIVO GENERAL	5
3. METAS DEL PROYECTO	5
4. FORMA DE PAGO	5
5. ALCANCE	5
6. TIEMPO DE ENTREGA.....	6
7. TIEMPO DE LOS BIENES Y SERVICIOS.....	6
8. BIENES Y SERVICIOS A ADQUIRIRSE Y SUS ESPECIFICACIONES.....	6
a) Herramientas Físicas de Ciberseguridad	6
i) Dispositivos de Autenticación Multifactor (MFA):	6
ii) Herramientas Físicas de Pen Testing y Análisis Forense	6
b) Equipo de Virtualización y Laboratorio de Ciberdefensa	7
c) Equipos de Telecomunicaciones.....	7
i) Firewall de próxima generación – 5 Unidades	7
ii) Sistema automatizado de protección, detección y respuesta (EDR) – 1 Unidad	7
iii) Switches Cisco Catalyst Layer 3– 15 Unidades	7
9. REQUERIMIENTOS ESPECÍFICOS	8
a) Capacitación Certificada	8
b) Requerimientos de Seguridad	8
10. REQUERIMIENTOS GENERALES	8
11. CONDICIONES GENERALES	8
12. CRITERIOS DE CONDICIONES DE PAGO	9
13. FACTURACIÓN Y CONDICIONES DE ENTREGA	9
15. CAPÍTULO: ENTREGA, INSTALACIÓN Y PUESTA EN MARCHA DE LOS EQUIPOS	9
1. OBJETIVO DEL CAPÍTULO	9
2. DESCRIPCIÓN GENERAL	9
3. REQUISITOS GENERALES DE ENTREGA E INSTALACIÓN	10
a) Entrega Física	10
b) Instalación en Sitio	10

c) Configuración Inicial	10
d) Pruebas Funcionales.....	10
e) Acta de Recepción Técnica	11
4. UBICACIONES DE INSTALACIÓN.....	11
5. DOCUMENTACIÓN DE SOPORTE	11
6. GARANTÍA POST-INSTALACIÓN	11
7. CRITERIOS DE ACEPTACIÓN FINAL.....	11
8. RESPONSABILIDADES DEL PROVEEDOR.....	12
9. RESPONSABILIDADES DE LA INSTITUCIÓN.....	12
10. CONSIDERACIONES ADICIONALES	12

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 registrará 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



MICHAEL ORTIZ
ADMINISTRADOR DE REDES



---Fin del Documento---