ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE EDUCACIÓN

ANEXO TÉCNICO SEGURIDAD PERIMETRAL 2026

REALIZAR LA RENOVACIÓN DEL LICENCIAMIENTO DE LA PLATAFORMA DE SEGURIDAD PERIMETRAL EXISTENTE Y ADQUIRIR LA SOLUCIÓN LAN, WIFI Y FIREWALL COMPATIBLE CON LA INFRAESTRUCTURA TECNOLÓGICA ACTUAL DE LA SECRETARÍA DE EDUCACIÓN DEL DISTRITO.



SECRETARÍA DE EDUCACIÓN DEL DISTRITO

BOGOTÁ – COLOMBIA

Versión 1.0
Septiembre~~Julio~~ 2026

Av. Eldorado No. 66 – 63
PBX: 324 10 00 Fax: 315 34 48
Código postal: 111321
www.educacionbogota.edu.co
Información: Línea 195

BOGOTÁ

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE EDUCACIÓN

TABLA DE CONTENIDO

1. OBJETO 4
2. ALCANCE DEL OBJETO 4
   - Fase 1. Renovación licenciamiento 4
   - Fase 2. Fortalecimiento red LAN 6
   - Fase 3. Fortalecimiento red WiFi CDI (Centro de Innovación) 6
   - Fase 4. Fortalecimiento Seguridad Perimetral NVC (Nivel Central) 7
   - Bolsa de horas Especializada 7
3. DETALLE TÉCNICO 7
   - 3.1. Fase 1 Renovación Licenciamiento 7
   - 3.2. Fase 2 Fortalecimiento Red LAN 10
   - 3.3. Fase 3 Fortalecimiento red WiFi CDI (Centro de Innovación) 11
   - 3.4. Fase 4 Fortalecimiento Seguridad Perimetral NVC (Nivel Central) 14
   - 3.5. Bolsa de Horas Especializada 14
4. FASES DEL CONTRATO 19
   - 4.1. Fase 1. Renovación licenciamiento 19
   - 4.2. Fase 2. Fortalecimiento red LAN 19
   - 4.2.1. Planeación 20
   - 4.2.2. Implementación 20
   - 4.2.3. Pruebas 21
   - 4.2.4. Criterios de Aceptación 23
   - 4.2.5. Entrega de la solución LAN en funcionamiento y licenciamiento activado 23
   - 4.2.6. Estabilización 23
   - 4.2.7. Certificación de cableado estructurado 24
   - 4.3. Fase 3. Fortalecimiento red WiFi CDI (Centro de Innovación) 24
   - 4.3.1. Planeación 25
   - 4.3.2. Implementación 25
   - 4.3.3. Entrega de la solución WiFi en funcionamiento y licenciamiento activado. 28
   - 4.3.4. Estabilización 28
   - 4.3.5. Certificación de cableado estructurado 29
   - 4.4. Fase 4. Fortalecimiento Seguridad Perimetral NVC (Nivel Central) 30

4.4.1. Planeación 30
4.4.2. Implementación 30
4.4.3. Pruebas 31
4.4.4. Entrega de Firewall en HA y Licenciamiento Activado 31
4.4.5. Estabilización 31
5. LUGAR DE ENTREGA 32
6. PLAZO DE EJECUCIÓN 32
7. CÓDIGOS UNSPSC 33
8. SERVICIOS DE SOPORTE DEL IMPLEMENTADOR 34
9. SERVICIOS DE SOPORTE CON FÁBRICA 35
10. TRANSFERENCIA DE CONOCIMIENTO (No Certificada) 36
11. NIVEL DE CERTIFICACIÓN O MEMBRESÍA DEL PROVEEDOR 36
12. CERTIFICACIÓN DE LA CASA MATRIZ, AUTORIZACIÓN DE COMERCIALIZACIÓN 36
13. ACUERDOS DE CONFIDENCIALIDAD 36

INDICE DE TABLAS

Tabla 1 Soluciones de seguridad perimetral implementadas en la SED 4
Tabla 2 Detalle técnico solución LAN 6
Tabla 3 Detalle técnico solución WiFi 6
Tabla 4 Detalle técnico solución Firewall 7
Tabla 1 Soluciones de seguridad perimetral implementadas en la SED 8
Tabla 2 Detalle técnico solución LAN 10
Tabla 3 Detalle técnico solución WiFi 11
Tabla 4 Detalle técnico solución Firewall 14
Tabla 5 Códigos UNSPSC 33

1. OBJETO

REALIZAR LA RENOVACIÓN DEL LICENCIAMIENTO DE LA PLATAFORMA DE SEGURIDAD PERIMETRAL EXISTENTE Y ADQUIRIR LA SOLUCIÓN LAN, WIFI Y FIREWALL COMPATIBLE CON LA INFRAESTRUCTURA TECNOLÓGICA ACTUAL DE LA SECRETARÍA DE EDUCACIÓN DEL DISTRITO.

2. ALCANCE DEL OBJETO

Para el desarrollo del objeto, el CONTRATISTA deberá atender los requerimientos de la entidad definidos en las siguientes 4 fases:

Fase 1. Renovación licenciamiento
Fase 2. Fortalecimiento red LAN
Fase 3. Fortalecimiento red WiFi CDI (Centro de Innovación)
Fase 4. Fortalecimiento Seguridad Perimetral NVC (Nivel Central)

Es importante precisar que, en atención a la estructura por fases, el alcance del presente proceso se encuentra articulado de manera integral, y que las especificaciones técnicas, actividades detalladas y condiciones particulares de ejecución de cada fase se encuentran definidas en el Anexo Técnico, el cual hace parte integral del proceso.

En este sentido, el Anexo Técnico constituye el documento de referencia para la comprensión completa del alcance, garantizando la correcta ejecución de cada una de las fases definidas.

- **Fase 1. Renovación licenciamiento**

La Secretaría de Educación del Distrito requiere contratar la renovación del licenciamiento de los equipos físicos y máquinas virtuales de Fortinet descritos en el Anexo Técnico. Esta renovación debe garantizar la continuidad operativa de la infraestructura de seguridad perimetral, la plena funcionalidad de los servicios actualmente implementados y el acceso al soporte directo de fábrica, incluyendo actualizaciones, mantenimiento, asistencia técnica especializada y demás componentes necesarios para asegurar la disponibilidad, integridad y protección de la plataforma tecnológica institucional, conforme a las especificaciones relacionadas en la tabla siguiente.

A continuación, se discriminan las soluciones objeto de renovación, indicando aquellas que aplican con IVA y aquellas que, por su naturaleza de servicios en la nube, se encuentran excluidas de este impuesto.

Tabla 1 Soluciones de seguridad perimetral implementadas en la SED

		#	Número Serial	Modelo	Descripción	Ubicación	Cantidad
LICENCIAMIENTO	SIN IVA	1	FADV040000226775	FortiADC VM04	ADC-SED-AZURE	Azure	1
		2	FGVM8VTM22000192	FortiGate VM08V	FWVM-SED-AZURE	Azure	1
		3	FGVM8VTM22000496	FortiGate VM08V	FWVM-SED-ORACLE	OCI	1
		4	FVVM04TM22000364	FortiWeb VM 4 CPU	WAF-SED-AZURE	Azure	1
		5	FVVM04TM22000633	FortiWeb VM 4 CPU	WAF-SED-ORACLE	OCI	1
	CON IVA	6	FAD12FT221000253	FortiADC 1200F	Balanceador_SED_CDI	CDI	1
		7	FAD12FT221000270	FortiADC 1200F	FortiADC-NVC-SED	NVC	1
		8	FAZ1KFTA20000140	FortiAnalyzer 1000F	FAZ-SED-CDI	CDI	1
		9	FE3K2ET320000001	FortiMail 3200E	FORTIMAIL-SED_CDI	CDI	1
		10	FE3K2ET321000004	FortiMail 3200E	FORTIMAIL SED NVC	NVC	1

	#	Número Serial	Modelo	Descripción	Ubicación	Cantidad
	11	FG180FTK21900625	FortiGate 1800F	SED-CDI_2	CDI	1
	12	FG180FTK21900952	FortiGate 1800F	SED-CDI_1	CDI	1
	13	FG180FTK21901353	FortiGate 1800F	SED-CTD_1	CTD	1
	14	FG180FTK25900403	FortiGate 1800F	SED_CTD_2	CTD	1
	15	FG180FTK21901434	FortiGate 1800F	SED-NVC_1	NVC	1
	16	FMG2HGTA21000190	FortiManager 200G	FMG-SED-CDI	CDI	1
	17	FSA1KFT619000161	FortiSandbox 1000F	FSA_SED-CDI	CDI	1
	18	FV-1KE4417900055	FortiWeb 1000E	F-WEB-SED-CDI	CDI	1
	19	FV-1KET122900059	FortiWeb 1000E	FortiWEB-CDI	CDI	1
	20	FP441KTF24015937	FortiAP 441K	NVC_Torre-A_Piso-4_Ubicacion-2	NVC	1
	21	FP441KTF24016047	FortiAP 441K	NVC_Torre-A_Piso-4_Ubicacion-7	NVC	1
	22	FP441KTF24016049	FortiAP 441K	NVC_Torre-A_Piso-4_Ubicacion-6	NVC	1
	23	FP441KTF24018106	FortiAP 441K	NVC_Torre-A_Piso-2_Ubicacion-1	NVC	1
	24	FP441KTF24018109	FortiAP 441K	NVC_Torre-A_Piso-4_Ubicacion-3	NVC	1
	25	FP441KTF24018115	FortiAP 441K	NVC_Torre-A_Piso-2_Ubicacion-2	NVC	1
	26	FP441KTF24019400	FortiAP 441K	NVC_Torre-A_Piso-3_Ubicacion-5	NVC	1
	27	FP441KTF24019405	FortiAP 441K	NVC_Torre-A_Piso-3_Ubicacion-2	NVC	1
	28	FP441KTF24019406	FortiAP 441K	NVC_Torre-A_Piso-3_Ubicacion-3	NVC	1
	29	FP441KTF24019410	FortiAP 441K	NVC_Torre-A_Piso-3_Ubicacion-4	NVC	1
	30	FP441KTF24019413	FortiAP 441K	NVC_Torre-A_Piso-3_Ubicacion-6	NVC	1
	31	FP441KTF24019420	FortiAP 441K	NVC_Torre-A_Piso-3_Ubicacion-1	NVC	1
	32	FP441KTF24019422	FortiAP 441K	NVC_Torre-A_Piso-4_Ubicacion-1	NVC	1
	33	FP441KTF24019427	FortiAP 441K	NVC_Torre-A_Piso-4_Ubicacion-5	NVC	1
	34	FP441KTF24019428	FortiAP 441K	NVC_Torre-A_Piso-4_Ubicacion-4	NVC	1
	35	FP441KTF25001348	FortiAP 441K	NVC	NVC	1
	36	FP441KTF25001028	FortiAP 441K	NVC	NVC	1
	37	FP441KTF25001069	FortiAP 441K	NVC	NVC	1
	38	FP441KTF25001084	FortiAP 441K	NVC	NVC	1
	39	FP441KTF25001098	FortiAP 441K	NVC	NVC	1
	40	FP441KTF25001346	FortiAP 441K	NVC	NVC	1
	41	FP441KTF25001078	FortiAP 441K	NVC	NVC	1
	42	FP441KTF25001085	FortiAP 441K	NVC	NVC	1
	43	FP441KTF25001095	FortiAP 441K	NVC	NVC	1
	44	FP441KTF25001202	FortiAP 441K	NVC	NVC	1
	45	FP441KTF25001114	FortiAP 441K	NVC	NVC	1
	46	FP441KTF25001094	FortiAP 441K	NVC	NVC	1
	47	FP441KTF25000877	FortiAP 441K	NVC	NVC	1
	48	FP441KTF25001344	FortiAP 441K	NVC	NVC	1
	49	FP441KTF25001058	FortiAP 441K	NVC	NVC	1
	50	FP441KTF25001075	FortiAP 441K	NVC	NVC	1
	51	FP441KTF25000369	FortiAP 441K	NVC	NVC	1
	52	FP441KTF25001079	FortiAP 441K	NVC	NVC	1
	53	FP441KTF25001097	FortiAP 441K	NVC	NVC	1
	54	FP441KTF25001198	FortiAP 441K	NVC	NVC	1
	55	FP441KTF25001076	FortiAP 441K	NVC	NVC	1
	56	FP441KTF25001086	FortiAP 441K	NVC	NVC	1
	57	FP441KTF25001302	FortiAP 441K	NVC	NVC	1
	58	FP441KTF25001029	FortiAP 441K	NVC	NVC	1
	59	FP441KTF25001103	FortiAP 441K	NVC	NVC	1
	60	FP441KTF25001115	FortiAP 441K	NVC	NVC	1
	61	FP441KTF25000948	FortiAP 441K	NVC	NVC	1
	62	FP441KTF25000979	FortiAP 441K	NVC	NVC	1
	63	FP441KTF25001204	FortiAP 441K	NVC	NVC	1
	64	FP441KTF25000811	FortiAP 441K	NVC	NVC	1
	65	FP441KTF25012991	FortiAP 441K	NVC	NVC	1
	66	FP441KTF24017562	FortiAP 441K	NVC	NVC	1
	67	S648FFTV25007304	Fortiswitch 648F-FPOE	NVC	NVC	1

		#	Número Serial	Modelo	Descripción	Ubicación	Cantidad
		68	S648FFTV25007305	Fortiswitch 648F-FPOE	NVC	NVC	1
		69	S648FFTV25007261	Fortiswitch 648F-FPOE	NVC	NVC	1
		70	S648FFTV24000389	Fortiswitch 648F-FPOE	NVC	NVC	1

CDI: Centro de Innovación Cra. 28a # 62-46
NVC: Nivel Central Av. Dorado # 66-63
AZURE: Nube publica de Microsoft
OCI: Oracle Cloud Infraestructure Nube publica de Oracle

El proponente deberá presentar precios para el licenciamiento de soluciones de seguridad perimetral Fortinet a un (1) año a partir de la suscripción del acta de inicio y no antes de la fecha de vencimiento del licenciamiento actual; asimismo, teniendo en cuenta aquellas soluciones en nube que están excluidas de IVA.

Nota**:** Para los equipos FortiMail 3200E (seriales **FE3K2ET320000001** y **FE3K2ET321000004**), el licenciamiento y soporte se renovarán únicamente hasta el **4 de mayo de 2027**, fecha en la cual finaliza el soporte de fábrica conforme a la política EOS (End of Service) del fabricante

- **Fase 2. Fortalecimiento red LAN**

Realizar la renovación tecnológica de la infraestructura de conmutación de red (switches de piso) de la sede de nivel Central de la SED, mediante la adquisición, instalación, configuración, integración, puesta en operación y soporte de switches de acceso, con el fin de modernizar, estandarizar y fortalecer la red institucional, garantizando su integración nativa con la solución de seguridad perimetral actual de la entidad, conforme a las especificaciones relacionadas en la tabla siguiente:

Tabla 2 Detalle técnico solución LAN

	#	DESCRIPCIÓN	Unidad de Medida	Cantidad
LAN	1	FORTISWITCH FS-148F	Unidad	1
	2	Switch FortiCare Premium Support	Unidad	1
	3	Servicio Instalación / implementación / Puesta en Marcha	Unidad	1

- **Fase 3. Fortalecimiento red WiFi CDI (Centro de Innovación)**

Realizar el fortalecimiento de la red WiFi en el Centro de Innovación (CDI), mediante la entrega, instalación y configuración de equipos de solución WiFi, integrándolos a la plataforma de seguridad perimetral existente de la entidad y validando que se mitiguen los riesgos identificados en el site survey realizado, conforme a las especificaciones relacionadas en la tabla siguiente:

Tabla 3 Detalle técnico solución WiFi

	#	DESCRIPCIÓN	Unidad de Medida	Cantidad
WiFi	1	FortiAP 231K Indoor indoor APs provide three radios and two spatial streams.	Unidad	6
	2	AP FortiCare Premium Support	Unidad	6

	3	FORTISWITCH 110G-FPOE Layer 2 FortiGate switch controller compatible PoE+ switch with 2x 5 GE ports with PoE 802.3bt, 8x 1GE RJ45 ports with PoE 802.3af/at, 4x 10 GE SFP+, Fanless with maximum 200W PoE output limit.	Unidad	1
	4	Switch FortiCare Premium Support	Unidad	1
	5	Puntos de red / Soporteria	Unidad	6
	6	Servicio Instalación / implementación / Puesta en Marcha	Unidad	6

- **Fase 4. Fortalecimiento Seguridad Perimetral NVC (Nivel Central)**

Realizar el fortalecimiento de la solución de seguridad perimetral del datacenter de NVC, mediante la entrega, instalación y configuración de un Firewall en HA (Alta disponibilidad) con el firewall existente, integrándolo en modo clúster a la plataforma de seguridad de la SED, conforme al detalle técnico relacionado en la tabla siguiente:

Tabla 4 Detalle técnico solución Firewall

#	Descripción	Unidad de Medida	Cantidad
1	Firewall Fortinet - Fortigate 1800F (Dispositivo físico) NVC	1	1

- **Bolsa de horas Especializada**

Contar con una bolsa de horas de ingeniería especializada en seguridad perimetral y redes inalámbricas (WiFi) que permita a la SED disponer de acompañamiento técnico continuo en actividades de administración, gestión, arquitectura, ajustes, traslados, renovaciones tecnológicas y resolución de incidentes sobre la plataforma Fortinet existente y las nuevas soluciones LAN, WiFi y Firewall a implementar, conforme al detalle relacionado en la tabla siguiente:

Tabla 5 Detalle paquete de Horas Especializadas

#	Descripción	Unidad de Medida	Cantidad
1	Ingeniero junior X Hora	1	10
2	Ingeniero Senior X Hora	1	10

3. DETALLE TÉCNICO

3.1. Fase 1 Renovación Licenciamiento

La Secretaría de Educación del Distrito requiere realizar la renovación compra de las licencias de los equipos físicos y máquinas virtuales de Fortinet descritas en este Anexo Técnico, que permitan su funcionalidad, al igual que el soporte directo de fábrica, según la tabla siguiente:

Tabla 5 Soluciones de seguridad perimetral implementadas en la SED

	#	Número Serial	Modelo	Descripción	Ubicación	Cantidad
LICENCIAMIENTO	1	FAD12FT221000253	FortiADC 1200F	FortiADC-CDI-SED	CDI	1
	2	FAD12FT221000270	FortiADC 1200F	FortiADC-NVC-SED	NVC	1
	3	FADV040000226775	FortiADC VM04	ADC-SED-AZURE	Azure	1
	4	FAZ1KFTA20000140	FortiAnalyzer 1000F	FAZ-SED-CDI	CDI	1
	5	FE3K2ET320000001	FortiMail 3200E	FORTIMAIL-SED_CDI	CDI	1
	6	FE3K2ET321000004	FortiMail 3200E	FORTIMAIL SED NVC	NVC	1
	7	FG180FTK21900625	FortiGate 1800F	SED-CDI_2	CDI	1
	8	FG180FTK21900952	FortiGate 1800F	SED-CDI_1	CDI	1
	9	FG180FTK21901353	FortiGate 1800F	SED-CTD_1	CTD	1
	10	FG180FTK25900403	FortiGate 1800F	SED_CTD_2	CTD	1
	11	FG180FTK21901434	FortiGate 1800F	SED-NVC_1	NVC	1
	12	FGVM8VTM22000192	FortiGate VM08V	FWVM-SED-AZURE	Azure	1
	13	FGVM8VTM22000496	FortiGate VM08V	FWVM-SED-ORACLE	OCI	1
	14	FMG2HGTA21000190	FortiManager 200G	FMG-SED-CDI	CDI	1
	15	FSA1KFT619000161	FortiSandbox 1000F	FSA_SED-CDI	CDI	1
	16	FV-1KE4417900055	FortiWeb 1000E	F-WEB-SED-CDI	CDI	1
	17	FV-1KET122900059	FortiWeb 1000E	FortiWEB-CDI	CDI	1
	18	FVVM04TM22000364	FortiWeb VM 4 CPU	WAF-SED-AZURE	Azure	1
	19	FVVM04TM22000633	FortiWeb VM 4 CPU	WAF-SED-ORACLE	OCI	1
	20	FP441KTF24015937	FortiAP 441K	NVC_Torre-A_Piso-4_Ubicacion-2	NVC	1
	21	FP441KTF24016047	FortiAP 441K	NVC_Torre-A_Piso-4_Ubicacion-7	NVC	1
	22	FP441KTF24016049	FortiAP 441K	NVC_Torre-A_Piso-4_Ubicacion-6	NVC	1
	23	FP441KTF24018106	FortiAP 441K	NVC_Torre-A_Piso-2_Ubicacion-1	NVC	1
	24	FP441KTF24018109	FortiAP 441K	NVC_Torre-A_Piso-4_Ubicacion-3	NVC	1
	25	FP441KTF24018115	FortiAP 441K	NVC_Torre-A_Piso-2_Ubicacion-2	NVC	1
	26	FP441KTF24019400	FortiAP 441K	NVC_Torre-A_Piso-3_Ubicacion-5	NVC	1
	27	FP441KTF24019405	FortiAP 441K	NVC_Torre-A_Piso-3_Ubicacion-2	NVC	1
	28	FP441KTF24019406	FortiAP 441K	NVC_Torre-A_Piso-3_Ubicacion-3	NVC	1
	29	FP441KTF24019410	FortiAP 441K	NVC_Torre-A_Piso-3_Ubicacion-4	NVC	1
	30	FP441KTF24019413	FortiAP 441K	NVC_Torre-A_Piso-3_Ubicacion-6	NVC	1
	31	FP441KTF24019420	FortiAP 441K	NVC_Torre-A_Piso-3_Ubicacion-1	NVC	1

	#	Número Serial	Modelo	Descripción	Ubicación	Cantidad
	32	FP441KTF24019422	FortiAP 441K	NVC_Torre-A_Piso-4_Ubicacion-1	NVC	1
	33	FP441KTF24019427	FortiAP 441K	NVC_Torre-A_Piso-4_Ubicacion-5	NVC	1
	34	FP441KTF24019428	FortiAP 441K	NVC_Torre-A_Piso-4_Ubicacion-4	NVC	1
	35	FP441KTF25001348	FortiAP 441K	NVC	NVC	1
	36	FP441KTF25001028	FortiAP 441K	NVC	NVC	1
	37	FP441KTF25001069	FortiAP 441K	NVC	NVC	1
	38	FP441KTF25001084	FortiAP 441K	NVC	NVC	1
	39	FP441KTF25001098	FortiAP 441K	NVC	NVC	1
	40	FP441KTF25001346	FortiAP 441K	NVC	NVC	1
	41	FP441KTF25001078	FortiAP 441K	NVC	NVC	1
	42	FP441KTF25001085	FortiAP 441K	NVC	NVC	1
	43	FP441KTF25001095	FortiAP 441K	NVC	NVC	1
	44	FP441KTF25001202	FortiAP 441K	NVC	NVC	1
	45	FP441KTF25001114	FortiAP 441K	NVC	NVC	1
	46	FP441KTF25001094	FortiAP 441K	NVC	NVC	1
	47	FP441KTF25000877	FortiAP 441K	NVC	NVC	1
	48	FP441KTF25001344	FortiAP 441K	NVC	NVC	1
	49	FP441KTF25001058	FortiAP 441K	NVC	NVC	1
	50	FP441KTF25001075	FortiAP 441K	NVC	NVC	1
	51	FP441KTF25000369	FortiAP 441K	NVC	NVC	1
	52	FP441KTF25001079	FortiAP 441K	NVC	NVC	1
	53	FP441KTF25001097	FortiAP 441K	NVC	NVC	1
	54	FP441KTF25001198	FortiAP 441K	NVC	NVC	1
	55	FP441KTF25001076	FortiAP 441K	NVC	NVC	1
	56	FP441KTF25001086	FortiAP 441K	NVC	NVC	1
	57	FP441KTF25001302	FortiAP 441K	NVC	NVC	1
	58	FP441KTF25001029	FortiAP 441K	NVC	NVC	1
	59	FP441KTF25001103	FortiAP 441K	NVC	NVC	1
	60	FP441KTF25001115	FortiAP 441K	NVC	NVC	1
	61	FP441KTF25000948	FortiAP 441K	NVC	NVC	1
	62	FP441KTF25000979	FortiAP 441K	NVC	NVC	1
	63	FP441KTF25001204	FortiAP 441K	NVC	NVC	1
	64	FP441KTF25000811	FortiAP 441K	NVC	NVC	1

	#	Número Serial	Modelo	Descripción	Ubicación	Cantidad
	65	FP441KTF25012991	FortiAP 441K	NVC	NVC	1
	66	FP441KTF24017562	FortiAP 441K	NVC	NVC	1
	67	S648FFTV25007304	Fortiswitch 648F-FPOE	NVC	NVC	1
	68	S648FFTV25007305	Fortiswitch 648F-FPOE	NVC	NVC	1
	69	S648FFTV25007261	Fortiswitch 648F-FPOE	NVC	NVC	1
	70	S648FFTV24000389	Fortiswitch 648F-FPOE	NVC	NVC	1

CDI: Centro de Innovación Cra. 28a # 62-46
NVC: Nivel Central Av. Dorado # 66-63
AZURE : Nube publica de Microsoft
OCI : Oracle Cloud Infrastructure Nube publica de Oracle

El proponente deberá presentar precios para el licenciamiento de soluciones de seguridad perimetral Fortinet a un (1) año a partir de la suscripción del acta de inicio, teniendo en cuenta aquellas soluciones en nube que están excluidas de IVA.

Nota: Para los equipos FortiMail 3200E (seriales **FE3K2ET320000001** y **FE3K2ET321000004**), el licenciamiento y soporte se renovarán únicamente hasta el **4 de mayo de 2027**, fecha en la cual finaliza el soporte de fábrica conforme a la política EOS (End of Service) del fabricante.

3.2. Fase 2 Fortalecimiento Red LAN

Conforme a las necesidades expuestas, surge la necesidad de adquirir:

Tabla 6 Detalle técnico solución LAN

	#	DESCRIPCIÓN	Unidad de Medida	Cantidad
LAN	1	FORTISWITCH FS-148F	Unidad	1
	2	Switch FortiCare Premium Support	Unidad	1
	3	Servicio Instalación / implementación / Puesta en Marcha	Unidad	1

Esta solución deberá cumplir con las siguientes características:

Switch FS-148F:

- Total, de interfaces de red: 48x GE RJ45 and 4x 10GE SFP+
- Capacidad de conmutación (dúplex): 176 Gbps
- Paquetes por segundo (dúplex): 260 Mbps
- Almacenamiento de direcciones MAC: 32 k
- Latencia de red: <1µs
- VLAN admitidas: 4 k
- Tamaño del grupo de agregación de enlaces: 8
- Total, de grupos de agregación de enlaces: 16
- Búferes de paquetes: 2 MB
- Memoria: 512 MB DDR3
- Flash: 64 MB
- Instancias Spanning Tree: 32

- Alimentación: 100–240V AC, 50-60 Hz
- Consumo (máximo): 55.8 W / 57 W
- Fuente de alimentación: AC built in
- Disipación de calor: 194.37 BTU/h
- Certificación y conformidad: FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2

3.3. Fase 3 Fortalecimiento red WiFi CDI (Centro de Innovación)

Conforme a las necesidades expuestas, surge la necesidad de adquirir:

Las cantidades definidas a continuación obedecen al estudio técnico llamado Site Survey descrito en el numeral 5. DESCRIPCIÓN DE LA NECESIDAD QUE SE PRETENDE SATISFACER CON LA CONTRATACIÓN Y ANÁLISIS DE CONVENIENCIA Y OPORTUNIDAD, Fase 3 Fortalecimiento red WiFi CDI, del Estudio Previo del presente proceso, el cual da soporte de las cantidades y tipos de soluciones a adquirir.

Tabla 7 Detalle técnico solución WiFi

	#	DESCRIPCIÓN	Unidad de Medida	Cantidad
WiFi	1	FortiAP 231K Indoor indoor APs provide three radios and two spatial streams.	Unidad	6
	2	AP FortiCare Premium Support	Unidad	6
	3	FORTISWITCH 110G-FPOE Layer 2 FortiGate switch controller compatible PoE+ switch with 2x 5 GE ports with PoE 802.3bt, 8x 1GE RJ45 ports with PoE 802.3af/at, 4x 10 GE SFP+, Fanless with maximum 200W PoE output limit.	Unidad	1
	4	Switch FortiCare Premium Support	Unidad	1
	5	Puntos de red / Soporteria	Unidad	6
	6	Servicio instalación / implementación / Puesta en Marcha	Unidad	6

Esta solución deberá cumplir con las siguientes características:

FAP 441K-A:

- Tipo
  - AP Interior
- Número de Antenas Interna: x4 WiFi doble banda +
  - 6. x2 Dual band Wi-Fi + x2 6GHz band Wi-Fi + x1 BLE/ ZigBee antenna + x1 GPS antenna
- Tipo de antena y ganancia máxima
  - PIFA 2.4/5GHz dual band antenna: 4.2 dBi for 2.4GHz, 5.0 dBi for 5 GHz
  - PIFA 6GHz antenna: 5.1 dBi for 6GHz band
  - PFA BLE antenna: 3.4 dBi for 2.
- Bandas de frecuencia (GHz).3
  - 2.4GHz Band:
    - ISM 2.4-2.484GHz
  - 5.0GHz Band:
    - UNII-1 5.15-5.25GHz,
    - UNII-2A 5.25-5.35GHz,

        - UNII-2C 5.47-5.73GHz,
        - UNII-3 5.725-5.85GHz,
        - UNII-4 5.85-5.895GHz
    - 6.0GHz Band:
        - UNII-5 5.925-6.425GHz,
        - UNII-6-6.425-6.525GHz,
        - UNII-7 6.525-6.875,
        - UNII-8 6.875-7.125GHz
- Capacidades Radio 1
    - Frequency band: 2.4GHz
    - Channel width: 20/40MHz
    - Modulation: BPSK, QPSK, 64/256/1024/4096 QAM
    - MIMO Chains: 2x2 Service
- Capacidades Radio 2
    - Frequency band: 5.0GHz UNII-1 to UNII-4
    - Channel width: 20/40/80/160MHz
    - Modulation: BPSK, QPSK, 16/64/256/1024/4096 QAM
    - MIMO Chains: 2x2 Service
- Capacidades Radio 3
    - Frequency band: 6.0GHz UNII-5 to UNII-8
    - Channel width: 20/40/80/160/320MHz
    - Modulation: BPSK, QPSK, 16/64/256/1024/4096 QAM
    - MIMO Chains: 2x2 Service
- Velocidad máxima de transmisión de datos
    - 2.4GHz band: up to 688 Mbps
    - 5.0GHz band: up to 2.882 Gbps
    - 6.0GHz band: up to 5.765 Gbps
- Bluetooth Low Energy
    - Bluetooth scanning and iBeacon advertizement @10 dBm max TX power
- GNSS
    - Bluetooth scanning and iBeacon advertizement
    - @10 dBm max TX power)
- Interfaces
    - x1 100M/1000M/2.5G/5.0G Multigigabit Ethernet (RJ45)
    - x1 RS-232 RJ45 Serial PortAlimentación a través de Ethernet (PoE)
- SSID simultáneos: Up to 8 per client serving radio (7 if background scanning is enabled)
- Tipo(s) EAP
    - EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST, EAP-TTLS/PAP
- Autenticación de usuario/dispositivo
    - WPA™, WPA2™, and WPA3™ with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blacklist and whitelist.
- Potencia máxima de transmisión (conducida)
    - 2.4GHz band: 26 dBm/400 mW (2 chains combined)*
    - 5.0GHz band: 23 dBm/200 mW (2 chains combined)*
    - 6.0GHz band: 22 dBm/158 mW (2 chains combined@320MHz BW)*
- Cerradura de Kensington
- Estándares IEEE

  - 802.11a, 802.11b, 802.11be, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11ac, 802.11ax, 802.11mc, 802.1X, 802.3af, 802.3at, 802.3bt, 802.3az, 802.1Q, 802.11u, 802.11w, 802.3bz
- Tipos de SSID admitidos
  - Local-Bridge, Mesh y Tunnel
- Capacidad de clientes por radio
  - Hasta 512 clientes por radio (Radio1, Radio2 y Radio3)
- Coexistencia celular
- Modo LED apagado
- Características 802.11 avanzadas
- OFDMA
- Reutilización espacial (BSS Coloring)
- UL MU-MIMO
- DL- MU-MIMO
- Fuente de alimentación: 802.3bt PoE: GPI-145 or 802.3at PoE: GPI-130 or 12V, 2.5A, 30 Watt DC power supply SP-FAP200-PA-XX
- Consumo (máx.): 15.2 W - PoE input 14.3 W - 12V DC power supply
- Modo PoE
  - 1. 802.3at: Tx Power - Full, 2x2 MIMO
  - 2. 802.3af : Tx Power- Full, 1x1 MIMO
- Humedad 5% a 90% sin condensación
- Temp. funcionamiento/almacenamiento
  - 32°F a 122°F (0°C a 50°C)/-22°F a 158°F (-30°C a 70°C)
- Directiva de Baja Tensión * RoHS
- UL2043 Material Plenum
- Tiempo Medio Entre Fallos >10 Años

Switch 110G-FPOE:

- Total, de interfaces de red
  - 2x 5G/2.5G/1G/100M
  - 8x 2.5G/1G/100M/10M RJ45
  - 4x 10G/1G/100 SFP+/SFP
- Puertos de consola serial: 1
- Puertos Power over Ethernet (PoE):
  - 2x 5G with PoE bt
  - 8x 2.5G with PoE af/at
- Capacidad de conmutación (dúplex): 140 Gbps
- Paquetes por segundo (dúplex): 208 Mpps
- Almacenamiento de direcciones MAC: 32 k
- Latencia de red: <1µs
- VLAN admitidas: 4 k
- Tamaño del grupo de agregación de enlaces: 10
- Total, de grupos de agregación de enlaces: 12
- Búferes de paquetes: 2 MB
- Memoria: 1GB DDR4
- Flash: 8 MB NOR

- Instancias Spanning Tree: 32
- Alimentación: 100-240 V CA, 50/60 Hz
- Consumo (máximo): 240 W
- Fuente de alimentación: 2x 350W
- Disipación de calor: 102.36 BTU/h
- Certificación y conformidad: FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2.

3.4. Fase 4 Fortalecimiento Seguridad Perimetral NVC (Nivel Central)

En el marco de la ejecución del contrato, el contratista deberá realizar la instalación de un (1) firewall para el Data Center ubicado en Nivel Central – NVC, Av. Dorado # 66-63, el cual debe ser 100% compatible con el Firewall existente y ser del mismo modelo físico, como se detalla a continuación:

Tabla 8 Detalle técnico solución Firewall

#	Descripción	Unidad de Medida	Cantidad
1	Firewall Fortinet - Fortigate 1800F (Dispositivo físico) NVC	1	1

El cual debe cumplir al menos los siguientes valores de desempeño:

- Desempeño de Firewall para IPv4 e IPv6: 198/197/140 Gbps
- Desempeño de VPN Ipsec: 55 Gbps
- Desempeño de VPN SSL: 11 Gbps
- Desempeño de Control de Aplicaciones: 34 Gbps
- Desempeño de NGFW: 17 Gbps
- Desempeño de IPS: 22 Gbps
- Desempeño de Threat Prevention: 15 Gbps
- Desempeño de inspección SSL: 12 Gbps
- Usuarios VPN SSL soportadas: 10.000
- Inspección de sesiones SSL concurrentes: 1.3 millones

El equipo FortiGate 1800F deberá ser suministrado con la suscripción FortiGuard Unified Threat Protection (UTP) o superior (Enterprise Protection), la cual deberá incluir como mínimo:

- Sistema de Prevención de Intrusiones (IPS)
- Antivirus / Antimalware
- Control de Aplicaciones
- FortiSandbox Cloud
- Filtrado Web y de Contenido
- Filtrado DNS seguro
- Filtrado de Video
- Protección Anti-Botnet y C2

El bundle UTP es el nivel mínimo exigido para garantizar la paridad funcional con el equipo existente (serial FG180FTK21901434), cuyo licenciamiento se renueva en la Fase 1. El proponente podrá ofertar el bundle Enterprise Protection como opción superior, pero en ningún caso se aceptarán niveles inferiores al UTP, toda vez que esto afectaría la operación del clúster HA y la funcionalidad de los servicios de seguridad.

El oferente debe entregar todos los conectores (transceiver), fibras ópticas, los cables y demás elementos

necesarios al momento de la entrega de los equipos, tanto para su conexión a la red LAN de la SED como para la creación del esquema HA High Availability).

El oferente deberá entregar los siguientes transceptores ópticos:

- Ocho (8) transceptores FN-TRAN-SFP28-SR (equivalente funcional al FN-TRAN-SFP-SR, doble velocidad 25 Gb/s y 10 Gb/s, 850 nm, fibra multimodo OM4, conector LC Dúplex, alcance 100 metros), distribuidos de la siguiente manera:
    - Cuatro (4) para uplinks LAN y WAN (redundancia y balanceo de carga).
    - Cuatro (4) para puertos dedicados a heartbeat/sincronización HA (alta disponibilidad).
- Cuatro (4) transceptores QSFP28/QSFP (100/40 Gbps) para interconexión de alta velocidad, cuya distribución será definida durante la etapa de implementación, previa coordinación con la OTIC.

Nota: El modelo **FN-TRAN-SFP-SR** especificado inicialmente es una referencia genérica; el transceptor exacto y equivalente del fabricante Fortinet es el **FN-TRAN-SFP28-SR**, el cual cumple con las especificaciones de doble velocidad (25 Gb/s y 10 Gb/s), 850 nm, 100 metros en fibra OM4 y conector LC Dúplex. Los transceptores entregados deberán ser **originales de Fortinet** y estar soportados oficialmente para el modelo FortiGate 1800F.

Para la interconexión del Firewall FortiGate 1800F con el Core de red del data center de NVC, la infraestructura de fibra óptica existente corresponde a fibra multimodo OM4. Los tramos entre el Firewall y el Core no superan los 20 metros de distancia. En consecuencia, los transceptores FN-TRAN-SFP28-SR requeridos deberán ser de alcance SR (Short Range), capaces de soportar distancias de hasta 20 metros sobre fibra OM4, lo cual es ampliamente cubierto por las especificaciones estándar de estos transceptores (hasta 100 metros en OM4).

3.5. Bolsa de Horas Especializada

La bolsa de horas especializadas constituye un mecanismo de disponibilidad técnica que permite a la SED acceder, bajo demanda y previa autorización del supervisor, a ingeniería certificada en seguridad perimetral y redes inalámbricas. Las 20 horas (10 junior + 10 senior) aquí previstas no pretenden cubrir en su totalidad la ejecución permanente de todas las actividades descritas a continuación, sino que están concebidas como una capacidad de respuesta ágil para atender necesidades específicas, críticas o no previstas dentro del alcance ordinario del contrato, tales como:

1. Arquitectura y evolución de la seguridad perimetral (Core de la solución)

1.1 Revisión y optimización del esquema de alta disponibilidad (HA)

- Actividad: Analizar la configuración actual del clúster HA en cada sitio (CDI, CTD, NVC) y en la nueva implementación del firewall en NVC.
- Detalle técnico:
    - Verificar modos HA activo-pasivo o activo-activo según el diseño.
    - Validar tiempos de conmutación (failover), sincronización de sesiones y consistencia de configuraciones.
    - Identificar y corregir asimetrías en políticas, objetos o rutas entre miembros del clúster.
    - Probar escenarios de falla simulada (pérdida de enlace, fallo de puerto, caída de proceso) y documentar RTO/RTO reales.

1.2 Diseño e implementación de segmentación de red avanzada

- Actividad: Definir e implementar una arquitectura de segmentación basada en zonas, VLANs y VDOMs (si aplica) para aislar tráfico crítico, administrativo, de invitados y de nube.
- Detalle técnico:
    - Crear zonas de seguridad (WAN, LAN, DMZ, Sync, Backup, Management, Cloud).
    - Configurar políticas de firewall entre zonas con inspección profunda (SSL, IPS, Application Control).
    - Implementar *Virtual Domains (VDOMs)* para separar operativamente entornos (ej. producción, pruebas, colegios).
        - Documentar matriz de flujos permitidos y denegados.

1.3 Integración de entornos cloud (Azure, OCI) con el Security Fabric

- Actividad: Asegurar que las máquinas virtuales FortiGate, FortiWeb y FortiADC en Azure y OCI estén plenamente integradas con la gestión centralizada y las políticas de seguridad.
- Detalle técnico:
    - Configurar túneles VPN IPsec site-to-site desde nubes a on-premise.
    - Habilitar *Fabric Connectors* para SDN (Azure/Oracle) y sincronizar etiquetas de recursos.
    - Implementar políticas consistentes entre nubes y datacenters físicos (mismos objetos, servicios, perfiles de seguridad).
    - Validar que el tráfico entre nubes se inspeccione correctamente sin bucles ni latencia excesiva.

2. Administración centralizada y orquestación (FortiManager / FortiAnalyzer)

2.1 Gestión unificada de políticas (FortiManager)

- Actividad: Centralizar, versionar y auditar todas las políticas de seguridad de los +70 equipos (on-premise, nube, colegios, DLE).
- Detalle técnico:
    - Crear Policy Packages por sitio/tipo de equipo y asignar a los dispositivos gestionados.
    - Implementar Install on Select Devices para despliegues selectivos.
    - Usar Global Policy para reglas comunes y Local Policy para excepciones.
    - Configurar workflows de aprobación de cambios (pre-validación, instalación, rollback).
    - Realizar auditorías periódicas de políticas huérfanas, sombras o redundantes.

2.2 Correlación de eventos y alertas proactivas (FortiAnalyzer)

- Actividad: Configurar dashboards, reportes automatizados y alertas basadas en anomalías de tráfico o intentos de intrusión.
- Detalle técnico:
    - Definir eventos críticos (cambios en HA, superación de umbrales de sesiones, actualizaciones fallidas, intentos de acceso no autorizados).
    - Configurar Event Handlers que disparen scripts, correos o tickets.
    - Crear reportes de cumplimiento (filtrado web, amenazas bloqueadas, aplicaciones usadas).
    - Integrar logs con SIEM corporativo si existe, mediante syslog o API.

2.3 Gestión de actualizaciones y parches de firmware

- Actividad: Planificar, probar y ejecutar actualizaciones de FortiOS y firmware de APs/switches en todo el parque.
- Detalle técnico:
    - Mantener una matriz de compatibilidad entre versiones (FortiGate, FortiAP, FortiSwitch, FortiManager, FortiAnalyzer).
    - Implementar un entorno de pruebas (staging) con equipos equivalentes antes del

despliegue en producción.
- Usar *FortiManager* para actualizaciones masivas programadas en ventanas de bajo impacto.
- Validar que después de la actualización las políticas, VPNs y HA sigan operando sin errores.

3. Operación avanzada de redes LAN y WiFi integradas

3.1 Configuración y afinamiento de switches FortiSwitch (LAN)

- Actividad: Implementar y optimizar la conmutación de acceso en NVC y CDI bajo el control del FortiGate (modo FortiLink).
- Detalle técnico:
  - Adoptar los switches en el FortiGate como *managed switches*.
  - Configurar VLANs de datos, voz, gestión, invitados y dispositivos IoT.
  - Aplicar políticas de acceso por puerto: autenticación 802.1X (con RADIUS), MAC bypass, o acceso estático.
  - Configurar *Storm Control*, *Loop Guard*, *BPDU Guard* y *DHCP Snooping* para proteger la capa 2.
  - Verificar que los uplinks de 10 Gbps sobre fibra OM4 operen sin errores CRC ni pérdidas.

3.2. Diseño y operación de red WiFi (FortiAP) post-site survey

- Actividad: Asegurar que la nueva solución WiFi en CDI cumpla y supere los parámetros del site survey predictivo/activo.
- Detalle técnico:
  - Configurar canales y potencia de transmisión evitando solapamiento (usar RRM o plan manual).
  - Implementar múltiples SSID con diferentes políticas de seguridad: WPA2-Enterprise, WPA3-Personal, portal cautivo.
  - Configurar *Band Steering* para desplazar clientes a 5/6 GHz.
  - Ajustar *Roaming* (802.11k/v/r) para sesiones sin cortes en movilidad.
  - Realizar un *post-implementation site survey* activo para medir SNR, throughput y cobertura real.

3.3. Integración de políticas de seguridad WiFi con el firewall

- Actividad: Asegurar que el tráfico inalámbrico se inspeccione igual que el cableado.
- Detalle técnico:
  - Asignar cada SSID a una VLAN y zona de seguridad específica.
  - Aplicar políticas de filtrado web, IPS y control de aplicaciones al tráfico WiFi.
  - Implementar *Captive Portal* con autenticación centralizada (RADIUS/LDAP) y términos de uso.
  - Configurar *Client Isolation* para evitar comunicación directa entre usuarios WiFi.

4. Soporte a proyectos de renovación, traslados y expansión

4.1 Acompañamiento en traslado o reubicación de equipos

- Actividad: Ejecutar el traslado físico y lógico de cualquiera de los equipos que componen la solución de seguridad perimetral de la entidad, switches o APs entre sedes (NVC, CDI, CTD, colegios, DLE) sin afectar la operación.
- Detalle técnico:
  - Realizar backup completo de configuración (incluyendo certificados, claves, objetos).
  - Documentar la topología pre-traslado y post-traslado.
  - Reconfigurar IPs, rutas, VLANs y políticas según la nueva ubicación.

- Validar conectividad con los sistemas centrales y la nube.
- Actualizar la gestión en FortiManager y los monitoreos.

4.2. Renovación de licenciamiento sin interrupción

- Actividad: Gestionar técnicamente la renovación anual de todas las suscripciones (UTM, FortiCare, etc.) para que no haya pérdida de servicio.
- Detalle técnico:
  - Verificar fechas de vencimiento de cada serial en la cuenta de soporte del fabricante.
  - Aplicar nuevas licencias (mediante archivos .lic o registro automático).
  - Confirmar que todos los servicios (Web Filter, IPS, Antivirus, FortiSandbox Cloud) se reactiven correctamente.
  - Documentar el estado de licenciamiento post-renovación.

5. Seguridad ofensiva defensiva y respuesta a incidentes

5.1 Pruebas de validación de controles de seguridad

Actividad: Ejecutar pruebas controladas para verificar que las políticas de seguridad mitigan las amenazas reales.

- Detalle técnico:
  - Utilizar herramientas como *Nmap*, *Metasploit* (en entorno autorizado)
  - Verificar que el IPS bloquea firmas críticas y que el firewall de aplicaciones web (FortiWeb) protege los servicios expuestos.
  - Comprobar que el filtrado web impide el acceso a categorías prohibidas.
  - Generar informes de brechas y recomendaciones de ajuste.

5.2. Análisis forense y respuesta a incidentes (post-ataque)

- Actividad: Investigar alertas de seguridad o incidentes reales utilizando logs del ecosistema Fortinet.
- Detalle técnico:
  - Correlacionar eventos desde FortiAnalyzer, FortiGate, FortiSandbox y FortiWeb.
  - Identificar el vector de ataque, el alcance y los indicadores de compromiso (IOCs).
  - Aislar equipos o segmentos afectados mediante políticas dinámicas o *Quarantine*.
  - Proponer y aplicar reglas de mitigación permanentes (bloqueo de IPs, dominios, hashes).
  - Documentar lecciones aprendidas y ajustar políticas.

5.3. Monitoreo proactivo de la superficie de ataque

- Actividad: Identificar servicios expuestos a internet (puertos, aplicaciones) que no deberían estarlo.
- Detalle técnico:
  - Usar *FortiGate* y *FortiAnalyzer* para listar todas las políticas NAT y ACLs entrantes.
  - Revisar reglas de acceso remoto (SSL VPN, IPsec) y aplicar controles de autenticación multifactor (MFA) si es posible.
  - Detectar servicios con cifrado débil o protocolos obsoletos (SSLv3, TLS 1.0).
  - Recomendar y ejecutar el cierre de servicios innecesarios.

6. Documentación, transferencia de conocimiento y acompañamiento a la OTIC

6.1 Elaboración de documentación técnica de arquitectura

- Actividad: Crear y mantener actualizada la documentación de la plataforma de seguridad perimetral y WiFi.

- Detalle técnico:
    - Diagramas de red lógica y física (con indicación de zonas, VLANs, enlaces, HA).
    - Matriz de políticas de firewall (origen, destino, servicio, acción, perfil de seguridad).
    - Inventario detallado de equipos (seriales, firmware, ubicación, licencias).
    - Procedimientos operativos estándar (SOP) para cambios comunes, respaldo y restauración.

6.2. Transferencia de conocimiento especializada (al personal de la OTIC)

- Actividad: Impartir sesiones prácticas y teóricas al equipo técnico de la SED sobre las soluciones Fortinet.
- Detalle técnico:
    - Talleres de administración diaria: políticas, objetos, monitoreo básico.
    - Sesiones avanzadas: troubleshooting con CLI, debugging de flujos, uso de *Flow Trace*.
    - Prácticas de respuesta a incidentes y análisis forense.
    - Entrenamiento en uso de FortiManager y FortiAnalyzer para reportes y auditoría.
    - Evaluación de conocimientos y certificación interna (no oficial) al final del acompañamiento.

6.3. Acompañamiento en comités de cambio y validación de impactos

- Actividad: Asistir a los comités de cambio técnico de la SED para evaluar el impacto de nuevas implementaciones, parches o migraciones.
- Detalle técnico:
    - Revisar los planes de cambio propuestos (por contratistas o internos).
    - Identificar riesgos de seguridad, disponibilidad o rendimiento.
    - Sugerir pruebas de validación y criterios de reversión (rollback).
    - Acompañar la ejecución de cambios críticos en horarios autorizados.

4. FASES DEL CONTRATO

El contrato contempla cuatro fases de ejecución en concordancia con el alcance establecido así:

Fase 1. Renovación licenciamiento
Fase 2. Fortalecimiento red LAN
Fase 3. Fortalecimiento red WiFi CDI (Centro de Innovación)
Fase 4. Fortalecimiento seguridad perimetral NVC (Nivel Central)

A continuación, se presenta el detalle del cumplimiento de cada fase:

4.1. Fase 1. Renovación licenciamiento

Para realizar la renovación anual del licenciamiento de los elementos de la plataforma de seguridad perimetral e interna instalada y en operación en los datacenter on-premise y cloud de la Secretaría de Educación del Distrito y definidos en la ***Tabla 1. Soluciones de seguridad perimetral implementadas en la SED***, deberá ser entregado y activado una vez suscrita el acta de inicio, se contempla un año de renovación de licenciamiento.

Nota: Para los equipos FortiMail 3200E (seriales **FE3K2ET320000001** y **FE3K2ET321000004**), el licenciamiento y soporte se renovarán únicamente hasta el **4 de mayo de 2027**, fecha en la cual finaliza el soporte de fábrica conforme a la política EOS (End of Service) del fabricante. En consecuencia, la oferta para estos dos (2) ítems deberá cubrir el licenciamiento y soporte únicamente hasta dicha fecha, sin incluir valores correspondientes a períodos posteriores. El valor de estos ítems corresponderá al ofertado por el proponente, sin exceder el precio techo de referencia establecido para cada uno.

La SED evaluará oportunamente las opciones de migración o reemplazo tecnológico para garantizar la continuidad del servicio.

4.2. Fase 2. Fortalecimiento red LAN

Para realizar el fortalecimiento de la red LAN del Nivel Central de la Entidad mediante la entrega, instalación y configuración de equipos de solución LAN, integrándolos a la plataforma de seguridad perimetral existente.

Elaborado un plan de trabajo que contempla el periodo de ejecución contractual para lo cual el contratista deberá incluir en su metodología las siguientes etapas:

- Planeación.
- Implementación, Instalación, configuración y puesta en producción de la solución LAN.
- Pruebas.
- Entrega de la solución LAN en funcionamiento y licenciamiento activado.
- Estabilización

Nota: El licenciamiento para la solución LAN adquirida por la entidad directo de fábrica empezara a regir a partir de la fecha de implementación y puesta en producción de esta.

4.2.1. Planeación

El contratista deberá incluir todos los costos asociados a la ejecución del proyecto, así como presentar un plan de trabajo que contemple las etapas de planeación, implementación, pruebas, puesta en operación y estabilización, el cual deberá ser aprobado por la supervisión del contrato. Deberá ser presentado dentro de los quince (15) días calendario siguientes a la suscripción del acta de inicio.

Dentro de los servicios el Contratista deberá realizar la Instalación, configuración y puesta en producción de las soluciones LAN ofertada, así como la entrega a satisfacción de estos a la entidad, realizando todas las tareas necesarias para cumplir con ello, sin que esto genere gastos o cobros adicionales para la entidad.

4.2.2. Implementación

Es responsabilidad del Contratista la puesta en producción de la solución LAN adquirida por la Entidad., toda vez que las pruebas realizadas hayan sido exitosas y dadas por aceptadas por el equipo técnico de la OTIC.

El Contratista deberá presentar a la Entidad la manera óptima en que realizará la implementación, en lo relacionado a priorización y los mejores momentos para realizar la implementación, a fin de lograr el menor impacto para el usuario final.

Dentro de los servicios, el Contratista debe tener en cuenta la Instalación, configuración y puesta en producción de la solución LAN ofertadas, así como la entrega a satisfacción de esta a la entidad, realizando todas las tareas necesarias para cumplir con ello y colocando el equipo técnico y de ingeniería necesario, sin que esto genere gastos o cobros adicionales para la entidad.

El contratista deberá incluir en su cotización todos los costos y gastos directos e indirectos asociados a la logística (Desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, papelería y comunicaciones) y todos los demás que sean requeridos para que el personal asignado al

proyecto pueda cumplir sus funciones y realizar las actividades contempladas en las fases descritas por la SED para la correcta ejecución del contrato.
El contratista deberá realizar la certificación del cableado estructurado correspondiente a cada punto de red instalado dentro del alcance del proyecto, en especial aquellos destinados a la conexión de Access Points (AP) y uplinks de switches.

Para la interconexión (uplink) de los switches de acceso con el Core de la red, la entidad informa que la infraestructura de fibra óptica existente corresponde a fibra multimodo OM4. En consecuencia, el contratista deberá garantizar la compatibilidad de los elementos suministrados con dicha infraestructura, incluyendo los transceptores SFP+ de 10 Gbps requeridos para la conexión de los switches a la red LAN.

Así mismo, el contratista deberá suministrar los patch cords de fibra óptica multimodo con conectores compatibles con los equipos a instalar (LC-LC o el tipo requerido según el diseño de interconexión), asegurando su adecuada categoría y calidad para soportar enlaces 10Gbps sobre fibra OM4, garantizando la estabilidad y correcto funcionamiento de los enlaces de uplink entre el NVC/Core de red y los switches de acceso.

4.2.3. Pruebas

La solución por implementar por el Contratista descrita en el presente documento y en sus anexos, deben ser probadas y validadas antes de su salida a producción. Para esto, se requiere que el Contratista realice de forma conjunta con el equipo técnico de la OTIC las pruebas de funcionalidad en un ambiente controlado que no comprometa la seguridad y disponibilidad de los servicios de los sistemas de información.

El Contratista deberá presentar el Plan de Pruebas que se realizará para la solución LAN requerida por la Entidad.

Durante la etapa de post-implementación y puesta en operación, el contratista deberá efectuar pruebas de seguridad, funcionamiento y operación, estas pruebas deberán ser validadas por la supervisión o a quien este designe, como requisito para el recibo a satisfacción de la solución. Para lo cual deberá acordar plan de trabajo con la Secretaría de Educación del Distrito, a través de la OTIC.

1. Pruebas de Funcionamiento Básico (Hardware y Software)
   1.1. Pruebas de Encendido y Estabilidad
      - Verificación de encendido correcto del equipo.
      - Validación de ausencia de alarmas críticas en el sistema.
      - Confirmación de operación estable durante un periodo mínimo de 48 horas continuas sin reinicios inesperados.
   1.2. Verificación de Firmware
      - Confirmación de instalación de la última versión estable y soportada del firmware.
      - Validación de compatibilidad del firmware con la solución de seguridad perimetral Fortinet actual de la entidad.
   1.3. Pruebas de Puertos y Interfaces
      - Validación de funcionamiento de todos los puertos Ethernet (uplink y acceso).
      - Verificación de negociación correcta de velocidad y dúplex.
      - Prueba de puertos PoE (cuando aplique): entrega de potencia, consumo y estabilidad.

2. Pruebas de Conectividad y Desempeño de Red
   2.1. Pruebas de Conectividad LAN
      - Verificación de conectividad entre dispositivos finales, switches de piso y core/distribución.

- Validación de comunicación entre VLANs según políticas definidas.

2.2. Pruebas de segmentación de red
Comprobación de correcta creación y operación de VLANs.
Validación de aislamiento entre segmentos según el diseño de red.
Pruebas de etiquetado (802.1Q) y propagación de VLANs.

2.3. Pruebas de Rendimiento

- Medición de latencia, pérdida de paquetes y throughput.
- Validación de desempeño bajo carga concurrente.
- Confirmación de operación sin congestión o cuellos de botella en escenarios normales de uso.

3. Pruebas de Integración con la Solución de Seguridad Perimetral Fortinet

3.1. Integración FortiSwitch – FortiGate

- Validación de adopción y administración del switch desde el FortiGate.
- Confirmación de operación en modo FortiLink.
- Verificación de sincronización de políticas y configuraciones.

3.2. Aplicación de Políticas de Seguridad

- Validación de aplicación de políticas de acceso por puerto.
- Pruebas de asignación dinámica de VLANs.
- Confirmación de control de tráfico basado en perfiles de seguridad.

3.3. Gestión Centralizada

- Verificación de visibilidad del switch desde FortiGate / FortiManager.
- Confirmación de monitoreo en tiempo real de puertos y dispositivos.
- Pruebas de administración centralizada sin acceso local directo al equipo.

4. Pruebas de Seguridad de Red (Capa 2 y Acceso).

4.1. Control de Acceso a la Red
Pruebas de autenticación de dispositivos (802.1X, cuando aplique).
Validación de comportamiento ante dispositivos no autorizados.
Confirmación de asignación de perfiles de acceso.

4.2. Protección de Capa 2

- Pruebas de mitigación de ataques de red (ARP poisoning, DHCP Attacks, MAC attacks y Spoofing Attacks).
- Validación de control de direcciones MAC por puerto.
- Confirmación de protección contra bucles de red (STP/RSTP/MSTP).

4.3. Seguridad Administrativa

- Verificación de deshabilitación de protocolos inseguros.
- Confirmación de acceso administrativo seguro (HTTPS, SSH).
- Validación de perfiles de usuario y roles de administración.

5. Pruebas de Alta Disponibilidad y Continuidad Operativa

5.1. Pruebas de Redundancia

- Validación de enlaces redundantes (uplinks).
- Pruebas de conmutación ante falla de enlace.
- Confirmación de continuidad del servicio durante eventos de falla simulados.

5.2. Pruebas de Recuperación

- Simulación de reinicio controlado del equipo.
- Validación de restauración de configuración.
- Confirmación de tiempos de recuperación aceptables.

6. Pruebas de Monitoreo, Registro y Auditoría
   6.1. Registro de Eventos
      - Verificación de generación de logs de eventos de red y seguridad.
      - Confirmación de envío de logs a FortiAnalyzer o sistema de monitoreo definido.
   6.2. Alertas y Notificaciones
      - Pruebas de alertas ante fallas de puertos, enlaces o dispositivos.
      - Validación de notificaciones por eventos críticos.
   6.3. Visibilidad y Reportes
      - Pruebas de alertas ante fallas de puertos, enlaces o dispositivos.
      - Validación de notificaciones por eventos críticos.
   6.4. Visibilidad y Reportes
      - Confirmación de visualización de estadísticas de tráfico.
      - Validación de reportes de uso y estado del equipo.

7. Pruebas de Gestión Operativa y Soporte
   7.1. Backup y Restauración
      - Prueba de respaldo de configuración.
      - Validación de restauración exitosa desde backup.
   7.2. Soporte y Licenciamiento
      - Verificación de activación de licencias correspondientes.
      - Confirmación de cobertura de soporte directo con fabrica.
      - Validación de acceso a actualizaciones y parches.

4.2.4. Criterios de Aceptación

Los switches de piso se considerarán recibidos a satisfacción cuando**:**

- Todas las pruebas descritas anteriormente hayan sido ejecutadas y documentadas.
- No se presenten fallas críticas o no conformidades abiertas.
- Se entregue informe técnico de pruebas, firmado por el contratista y avalado por la supervisión o a quien este delegue.
- Se garantice la operación integrada con la solución de seguridad perimetral Fortinet.

4.2.5. Entrega de la solución LAN en funcionamiento y licenciamiento activado

Es responsabilidad del Contratista realizar la entrega de la solución LAN implementada y el licenciamiento activado por un año.

4.2.6. Estabilización

El contratista deberá realizar y documentar entre otras, las siguientes actividades previa coordinación con el supervisor del contrato en desarrollo:

- Revisar y afinar la plataforma LAN implementada.
- Hacer uso de las herramientas de detección, diagnóstico y resolución de novedades que ayuden a conservar la estabilidad y óptimo rendimiento de la plataforma implementada.
- Configurar, afinar y revisar los reportes / logs de la plataforma implementada.
- Mantener actualizados los niveles de Firmware de las plataformas implementadas de acuerdo con
- las últimas versiones estables liberadas por el fabricante.
- El contratista deberá garantizar soportes correctivos sobre la solución implementada en la entidad de acuerdo con las fechas y horarios que la entidad determine.
- Al finalizar cada visita correctiva y/o preventiva el contratista deberá:

- Generar un informe de servicio en el que se realice un resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones.
- El contratista deberá consignar en el mismo informe de servicio si hubo cambio de software y/o en la configuración.

Adelantar el afinamiento y estabilización del firmware y todas las funcionalidades de la plataforma licenciada, estas actividades se deben desarrollar al inicio del contrato y durante su ejecución, si es requerido.

4.2.7. Certificación de cableado estructurado

Con el fin de garantizar el adecuado desempeño de la infraestructura de red que soportará los servicios de conectividad LAN y la operación de Access Points para redes inalámbricas bajo estándar WiFi 6 o superior, el contratista deberá asegurar que el cableado estructurado instalado cumpla con las especificaciones técnicas de Categoría 6A.

Para tal efecto, el contratista deberá realizar la certificación de cada punto de red instalado, incluyendo los destinados a la conexión de Access Points (AP), equipos de usuario y uplinks de switches, conforme a lo establecido en el estándar ANSI/TIA-568 vigente.

La certificación deberá efectuarse mediante un equipo certificador de cableado estructurado debidamente calibrado (por ejemplo, equipos de Fluke Networks o equivalente), aplicando pruebas de Permanent Link o su equivalente técnico.
Los reportes de certificación deberán evidenciar el cumplimiento de los parámetros exigidos para Categoría 6A, incluyendo como mínimo los siguientes:

- Wiremap
- Longitud del enlace
- Insertion Loss (Atenuación)
- Return Loss (Pérdida de retorno)
- NEXT (Near-End Crosstalk)
- PSNEXT (Power Sum NEXT)
- ACR-F / ELFEXT
- PSACR-F
- Delay
- Delay Skew

Cada reporte deberá indicar claramente el resultado de la prueba (PASS/FAIL) conforme a los límites definidos por el estándar aplicable.

Como parte de los entregables del contrato, el contratista deberá suministrar a la entidad:

- Los reportes completos de certificación por cada punto de red, en formato digital.
- La identificación del punto certificado, ubicación física, fecha de prueba y equipo utilizado.
- La evidencia de calibración vigente del equipo certificador utilizado para las pruebas.

La entrega de estos reportes constituirá requisito para la aceptación técnica del cableado estructurado instalado por parte de la entidad.

4.3. Fase 3. Fortalecimiento red WiFi CDI (Centro de Innovación)

Para realizar el fortalecimiento de la red WiFi de Centro de Innovación de la Entidad mediante el entrega, instalación y configuración de equipos de solución WiFi, integrándolos a la plataforma de seguridad existente y validando que se mitiguen los riesgos identificados en el site survey (estudio y dimensionamiento en sitio) elaborado en la entidad se contempla el periodo de ejecución contractual para lo cual el contratista deberá incluir en su metodología las siguientes etapas:

- Planeación.
- Implementación, Instalación, configuración y puesta en producción de la solución WiFi.
- Pruebas.
- Entrega de la solución WiFi en funcionamiento y licenciamiento activado.
- Estabilización.

Nota: El licenciamiento para la solución WiFi adquirida por la entidad directo de fabrica empezara a regir a partir de la fecha de implementación y puesta en producción de esta.

4.3.1. Planeación

El contratista deberá contemplar en su oferta todos los costos y gastos directos e indirectos asociados a la logística (Desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, papelería y comunicaciones) y todos los demás que sean requeridos para que el personal asignado al proyecto pueda cumplir sus funciones y realizar las actividades contempladas en las fases descritas por la SED para la correcta ejecución del contrato.
De igual manera se deberá presentar un plan de implementación, con cumplimiento durante la ejecución contractual, en el que incluya los pre-requisitos, el equipo de trabajo y los tiempos estimados. El plan de trabajo deberá tener presente las etapas de entrega, preparación, pruebas, puesta en producción y acompañamiento posterior (Post-implementación). El plan de trabajo deberá ser presentado dentro de los primeros quince (15) días calendario, para ser aprobado por el supervisor del contrato y a quien este delegue.
Dentro de los servicios el Contratista deberá realizar la Instalación, configuración y puesta en producción de las soluciones WiFi ofertada, así como la entrega a satisfacción de estos a la entidad, realizando todas las tareas necesarias para cumplir con ello, sin que esto genere gastos o cobros adicionales para la entidad. Esto incluye la corrección a conformidad de las necesidades identificadas durante el Site Survey tales como solapamiento de banda, Falta de cobertura en algunas zonas y Bajos valores de SNR: Desconexiones, pérdida de paquetes, reducción de velocidad y conexiones inestables.

4.3.2. Implementación

Es responsabilidad del Contratista la puesta en producción de la solución WiFi adquirida por la Entidad., toda vez que las pruebas realizadas hayan sido exitosas y dadas por aceptadas por el equipo técnico de la OTIC.

El Contratista deberá presentar a la Entidad la manera óptima en que realizará la implementación, en lo relacionado a priorización y los mejores momentos para realizar la implementación, a fin de lograr el menor impacto para el usuario final.

Dentro de los servicios, el Contratista debe tener en cuenta la Instalación, configuración y puesta en producción de la solución WiFi ofertadas, así como la entrega a satisfacción de esta a la entidad, realizando todas las tareas necesarias para cumplir con ello y colocando el equipo técnico y de ingeniería necesario, sin que esto genere gastos o cobros adicionales para la entidad.

El contratista deberá incluir en su cotización todos los costos y gastos directos e indirectos asociados a la logística (Desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, papelería y comunicaciones) y todos los demás que sean requeridos para que el personal asignado al proyecto pueda cumplir sus funciones y realizar las actividades contempladas en las fases descritas por la SED para la correcta ejecución del contrato.

Se debe realizar la creación, implementación y puesta en producción de un (1) portales cautivos, bajo los siguientes lineamientos técnicos, de seguridad y compatibilidad:

a. Características Técnicas

Elemento	Detalles
Infraestructura de red	WiFi con puntos de acceso (APs) gestionados centralmente, con soporte para múltiples SSID.
Portal cautivo	Plataforma de autenticación basada en web para controlar el acceso a la red inalámbrica.
Segmentación de red	VLAN separada: para **usuarios** invitados**.**
Redireccionamiento	Acceso inicial redirige a una URL de autenticación segura (HTTPS), bajo certificado seguro proveído por la SED.
Soporte multi dispositivo	Compatibilidad con laptops, smartphones y tablets con navegadores actuales.
Alta disponibilidad	Balanceo de carga y redundancia para evitar caídas del servicio.
Duración de sesión	Configuración de tiempos de sesión y reconexión automática para mejorar la experiencia de usuario.

b. Características de Seguridad

- Invitados
  - Control de acceso: restringidos a internet únicamente.
  - Login: mediante correo, código temporal o SMS (autenticación de uso limitado).
- Encriptación del tráfico: Uso obligatorio de HTTPS en el portal y WPA2/WPA3 en la red inalámbrica.
- Monitoreo y logs: Registro de accesos, dispositivos conectados y duración de sesión, cumpliendo normativas de privacidad.
- Políticas de uso aceptable (PUA): Aceptación obligatoria de términos y condiciones antes del acceso (definido y aprobado por la SED).
- Detección de amenazas: Integración con sistemas de detección de intrusos (IDS) y protección contra ataques MITM.
- Actualizaciones y parches: Mantenimiento continuo del sistema y firmware de los APs.

c. Características de Compatibilidad

Elemento	Detalles
Compatibilidad de navegador	Funcionalidad en navegadores modernos (Chrome, Firefox, Safari, Edge).
SO soportados	Windows, macOS, iOS, Android, Linux.
Soporte de idioma	Interfaz multilingüe (mínimo en español e inglés).
Diseño adaptativo	Portal web adaptable a dispositivos móviles.
Interoperabilidad	Integración con sistemas de gestión de identidad (IDM), firewalls, y proxies institucionales.

Los requerimientos técnicos y de seguridad definidos anteriormente serán, evaluados y aceptados por el equipo técnico de la SED a través de la OTIC.

d. Pruebas

La solución por implementar por el Contratista descrita en el presente documento y en sus anexos, deben ser probadas y validadas antes de su salida a producción. Para esto, se requiere que el Contratista realice de forma conjunta con el equipo técnico de la OTIC las pruebas de funcionalidad en un ambiente controlado que no comprometa la seguridad y disponibilidad de los servicios de los sistemas de información.

El Contratista deberá presentar el Plan de Pruebas que se realizará para la solución WiFi requerida por la Entidad.

Durante la etapa de post-implementación, el contratista deberá efectuar mínimo dos (2) pruebas sobre el servicio de la plataforma WiFi objeto del contrato, para lo cual deberá acordar plan de trabajo con la Secretaría de Educación del Distrito, a través de la OTIC. Estas pruebas se deberán realizar, como mínimo, en los siguientes contextos:

- Las pruebas de funcionalidad evalúan la capacidad de la red para funcionar correctamente:
  - Rendimiento:
    - Medir velocidad de subida y bajada (ej. con herramientas como iPerf, Speedtest).
    - Test de carga: cuántos dispositivos pueden conectarse sin perder rendimiento.
    - Verificar latencia, jitter y pérdida de paquetes.
  - Cobertura:
    - Evaluar la señal en distintos puntos del área, pisos y zonas.
    - Identificar zonas muertas o con señal débil.
  - Cambio de bandas (band steering):
    - Comprobar que los dispositivos cambian automáticamente entre 2.4 GHz y 5 GHz según la calidad de la señal.
  - Roaming:
    - Verificar que al moverse entre puntos de acceso (APs), los dispositivos no pierden la conexión.
  - Conectividad:
    - Comprobar que los dispositivos pueden conectarse a la red.
    - Verificar si el DHCP asigna IPs correctamente.
    - Confirmar acceso a internet y a recursos internos.
  - Pruebas de Seguridad (Security Testing): las pruebas de seguridad deberán evaluar.
  - Configuración del cifrado:
    - Verificar que se utilice WPA2 o WPA3 (evitar WEP/WPA).
    - Comprobar contraseñas seguras.
  - Prueba de autenticación:
    - Comprobar que sólo usuarios autorizados acceden a la red (MAC filtering, portal cautivo, RADIUS si aplica).
  - Pruebas de sniffing:
    - Utilizar herramientas como Wireshark para detectar si se puede interceptar tráfico en la red.
    - Probar si hay tráfico en texto plano (sin cifrar).
  - Pruebas de fuerza bruta:
    - Intentar romper contraseñas del WiFi (con cuidado y solo en entornos de prueba o con permiso).
  - Pruebas de aislamiento de clientes:

        - Verificar que los dispositivos conectados no puedan comunicarse entre sí (Client Isolation, AP Isolation).
    - Detección de puntos de acceso maliciosos:
        - Usar herramientas como Kismet o Acrylic Wi-Fi para encontrar APs falsos (Evil Twins).

El contratista deberá presentar informe de ejecución y resultado exitoso de las pruebas; informe de optimización realizada frente a los riesgos identificados en el site survey realizado, adicionalmente el informe debe contener propuestas de mejora o afinamiento para cada uno de los tópicos revisados.

La entidad será la responsable, a través de la OTIC, a través del supervisor del contrato y a quien este delegue de dar por aceptadas las pruebas y aquellas que la entidad considere que no cumple los propósitos técnicos definidos en el presente documento no serán aceptadas y estas deberán volver a realizarse.

Para la interconexión (uplink) de los switches de acceso con el Core de la red, la entidad informa que la infraestructura de fibra óptica existente corresponde a fibra multimodo OM4. En consecuencia, el contratista deberá garantizar la compatibilidad de los elementos suministrados con dicha infraestructura, incluyendo los transceptores SFP+ de 10 Gbps requeridos para la conexión de los switches a la red LAN. Así mismo, el contratista deberá suministrar los patch cords de fibra óptica multimodo con conectores compatibles con los equipos a instalar (LC-LC o el tipo requerido según el diseño de interconexión), asegurando su adecuada categoría y calidad para soportar enlaces 10Gbps sobre fibra OM4, garantizando la estabilidad y correcto funcionamiento de los enlaces de uplink entre el NVC/Core de red y los switches de acceso.

4.3.3. Entrega de la solución WiFi en funcionamiento y licenciamiento activado.

Es responsabilidad del Contratista realizar la entrega de la solución WiFi-implementada y el licenciamiento activado por un año.

4.3.4. Estabilización.

El contratista deberá realizar y documentar entre otras, las siguientes actividades previa coordinación con el supervisor del contrato en desarrollo:

- Revisar y afinar las plataforma WiFi implementada.
- Hacer uso de las herramientas de detección, diagnóstico y resolución de novedades que ayuden a conservar la estabilidad y óptimo rendimiento de la plataforma implementada.
- Configurar, afinar y revisar los reportes / logs de la plataforma implementada.
- Mantener actualizados los niveles de Firmware de las plataformas implementadas de acuerdo con las últimas versiones estables liberadas por el fabricante.
- El contratista deberá realizar soportes preventivos en sitio sobre los equipos implementados de la solución WiFi, sin costo adicional para la entidad y con una periodicidad trimestral durante la vigencia del contrato. La OTIC, a través del supervisor del contrato y a quien este delegue dará la aprobación para la realización de esta actividad, la cual incluye:

    - Verificación de estado de enlaces inalámbricos (backhaul, si aplica)
    - Revisión del uso del espectro y canales para evitar interferencias.
    - Monitorización de rendimiento (latencia, throughput, pérdida de paquetes).
    - Inspección visual rápida de puntos de acceso (AP) accesibles: LED, suciedad,

ventilación.
    - Reinicio programado de dispositivos por Actualización de firmware o software crítico, si es necesario y lo solución lo requiere. Esta actividad se realizará bajo aprobación de comité de cambios si es requerida.
    - Verificación de balanceo de carga entre APs y controladores.

- El contratista deberá garantizar soportes correctivos sobre la solución implementada en la entidad de acuerdo con las fechas y horarios que la entidad determine.
- Al finalizar cada visita correctiva y/o preventiva el contratista deberá:

    - Generar un informe de servicio en el que se realice un resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones.
    - El contratista deberá consignar en el mismo informe de servicio si hubo cambio de software y/o en la configuración.

Adelantar el afinamiento y estabilización del firmware y todas las funcionalidades de la plataforma licenciada, estas actividades se deben desarrollar al inicio del contrato y durante su ejecución, si es requerido.

4.3.5. Certificación de cableado estructurado

Con el fin de garantizar el adecuado desempeño de la infraestructura de red que soportará los servicios de conectividad LAN y la operación de Access Points para redes inalámbricas bajo estándar WiFi 6 o superior, el contratista deberá asegurar que el cableado estructurado instalado cumpla con las especificaciones técnicas de Categoría 6A.

Para tal efecto, el contratista deberá realizar la certificación de cada punto de red instalado, incluyendo los destinados a la conexión de Access Points (AP), equipos de usuario y uplinks de switches, conforme a lo establecido en el estándar ANSI/TIA-568 vigente.

La certificación deberá efectuarse mediante un equipo certificador de cableado estructurado debidamente calibrado (por ejemplo, equipos de Fluke Networks o equivalente), aplicando pruebas de Permanent Link o su equivalente técnico.

Los reportes de certificación deberán evidenciar el cumplimiento de los parámetros exigidos para Categoría 6A, incluyendo como mínimo los siguientes:

- Wiremap
- Longitud del enlace
- Insertion Loss (Atenuación)
- Return Loss (Pérdida de retorno)
- NEXT (Near-End Crosstalk)
- PSNEXT (Power Sum NEXT)
- ACR-F / ELFEXT
- PSACR-F
- Delay
- Delay Skew

Cada reporte deberá indicar claramente el resultado de la prueba (PASS/FAIL) conforme a los límites definidos por el estándar aplicable.

Como parte de los entregables del contrato, el contratista deberá suministrar a la entidad:

- Los reportes completos de certificación por cada punto de red, en formato digital.
- La identificación del punto certificado, ubicación física, fecha de prueba y equipo utilizado.
- La evidencia de calibración vigente del equipo certificador utilizado para las pruebas.

La entrega de estos reportes constituirá requisito para la aceptación técnica del cableado estructurado instalado por parte de la entidad.

4.4. Fase 4. Fortalecimiento Seguridad Perimetral NVC (Nivel Central)

Para realizar el fortalecimiento de la solución de seguridad perimetral SED ubicado en Nivel Central – NVC, Av. Dorado # 66-63, mediante la entrega, instalación y configuración de Firewall en HA (Alta disponibilidad) con el firewall existente e integrándolo a la plataforma de seguridad, se contempla el periodo de ejecución contractual, para lo cual el contratista deberá incluir en su metodología las siguientes etapas:

- Planeación.
- Implementación, Instalación, configuración y puesta en producción de la solución de seguridad perimetral - Firewall en HA (Alta Disponibilidad)
- Entrega de Firewall en HA y licenciamiento activado
- Pruebas
- Estabilización

4.4.1. Planeación

El contratista deberá contemplar en su oferta todos los costos y gastos directos e indirectos asociados a la logística (Desplazamiento, transporte, parqueaderos, equipos y herramientas de trabajo, refrigerios, papelería y comunicaciones) y todos los demás que sean requeridos para que el personal asignado al proyecto pueda cumplir sus funciones y realizar las actividades contempladas en las fases descritas por la SED para la correcta ejecución del contrato. De igual manera se deberá presentar un plan de implementación, que contemple su cumplimiento dentro del periodo de ejecución contractual en el que incluya los pre-requisitos, el equipo de trabajo y los tiempos estimados. El plan de trabajo deberá tener presente las etapas de entrega, preparación, pruebas, puesta en producción y acompañamiento posterior (Post-implementación). El plan de trabajo deberá ser aprobado por el equipo técnico de la OTIC, a través del supervisor del contrato y a quien este delegue. El futuro contratista deberá presentar su plan de trabajo basado en un cronograma, dentro de los primeros 15 días calendario el cual deberá ser aprobado por la OTIC. Dentro de los servicios el Contratista deberá realizar la Instalación, configuración y puesta en producción de la solución de Firewall ofertada, así como la entrega a satisfacción de estos a la entidad, realizando todas las tareas necesarias para cumplir con ello, sin que esto genere gastos o cobros adicionales para la entidad.

4.4.2. Implementación

Es responsabilidad del Contratista la puesta en producción de la solución de seguridad perimetral (Firewall), adquirida por la entidad en NVC (Nivel Central), en un esquema de HA junto con un Firewall de las mismas especificaciones técnicas, modelo y marca ya en operación.

El Contratista deberá presentar a la Entidad la manera óptima en que realizará la implementación, en lo

relacionado a priorización y los mejores momentos para realizar la implementación, a fin de lograr el menor impacto para el usuario final.

Dentro de los servicios, el Contratista debe tener en cuenta la Instalación, configuración y puesta en producción del Firewall adquirido por la entidad, así como la entrega a satisfacción de esta, realizando todas las tareas necesarias para cumplir con ello y colocando el equipo técnico y de ingeniería necesario, sin que esto genere gastos o cobros adicionales para la entidad.

4.4.3. Pruebas

La solución de seguridad perimetral (Firewall) por implementar por el Contratista descritas en el presente documento y en sus anexos, deben ser probadas y validadas antes de su salida a producción. Para esto, se requiere que el Contratista realice de forma conjunta con el equipo técnico de la OTIC las pruebas de funcionalidad en un ambiente controlado que no comprometa la seguridad y disponibilidad de los servicios de los sistemas de información.

El Contratista deberá presentar el Plan de Pruebas que se realizará para la solución de Firewall requerida por la Entidad.

Durante la etapa de post-implementación, el contratista deberá efectuar mínimo tres (3) pruebas sobre el servicio de seguridad perimetral (Firewall) objeto del contrato, las pruebas deberán garantizar:

- Formación del cluster HA
- Cambio de roles de Master-slave y Slave-Master
- Firewall asume, procesa y gestiona todo el trafico

Para lo cual deberá acordar plan de trabajo con la Secretaría de Educación del Distrito a través de la OTIC.

La entidad será la responsable, a través del SUPERVISOR de dar por aceptadas las pruebas y aquellas que la entidad considere que no cumple los propósitos técnicos definidos en el presente, documento no serán aceptadas y estas deberán volver a realizarse.

4.4.4. Entrega de Firewall en HA y Licenciamiento Activado

Es responsabilidad del Contratista realizar la entrega del Firewall configurado en HA (Alta disponibilidad y el licenciamiento activado por un año.

4.4.5. Estabilización

El contratista deberá realizar y documentar, entre otras, las siguientes actividades previa coordinación con el supervisor del contrato en desarrollo:

- Revisar y afinar la plataforma Firewall.
- Hacer uso de las herramientas de detección, diagnóstico y resolución de novedades que ayuden a conservar la estabilidad y óptimo rendimiento de la plataforma implementada.
- Configurar, afinar y revisar los reportes / logs de la plataforma implementada.
- Mantener actualizados los niveles de Firmware de las plataformas implementadas de acuerdo con las últimas versiones estables liberadas por el fabricante.
- El contratista deberá garantizar soportes correctivos sobre la solución implementada en la entidad de acuerdo con las fechas y horarios que la entidad determine.

- Al finalizar cada visita correctiva y/o preventiva el contratista deberá:
    - Generar un informe de servicio en el que se realice un resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones.
    - El contratista deberá consignar en la misma acta o informe de servicio si hubo cambio de software y/o en la configuración.

Adelantar el afinamiento y estabilización del firmware y todas las funcionalidades de la plataforma licenciada, estas actividades se deben desarrollar al inicio del contrato y durante su ejecución, si es requerido.

5. LUGAR DE ENTREGA

Los productos definidos en el presente documento deberán ser entregados en los siguientes lugares conforme a su ubicación:

- **Licenciamiento**: El licenciamiento deberá ser activado, conforme a la ubicación definida en la tabla1 ***Soluciones de seguridad perimetral implementadas en la SED***, así:
    - CDI Centro de Innovación Cra. 28a # 62-46
    - NVC Nivel Central Av. Dorado # 66-63
    - CTD Centro de Transformación Digital Calle 17 # 68 - 83 Zona Industrial Montevideo.
    - Azure
    - OCI

- **LAN**: la solución definida en la tabla 2 ***Detalle técnico solución LAN*** será puesto en producción en la sede de NVC Nivel Central Av. Dorado # 66-63.

- **WiFi:** la solución definida en la tabla 3 ***Detalle técnico solución WiFi*** será puesto en producción en la sede de NVC Nivel Central Av. Dorado # 66-63.

- **Firewall**: la solución definida en la tabla 4 ***Detalle técnico solución Firewall*** será puesto en producción en la sede NVC Nivel Central Av. Dorado # 66-63.

- **Bolsa de horas especializada**: Las horas de ingeniería especializada se ejecutarán bajo demanda en cualquiera de las ubicaciones donde la SED tenga infraestructura tecnológica activa, incluyendo Nivel Central (Av. Dorado #66-63), Centro de Innovación (Carrera 28a #62-46), Centro de Transformación Digital (Calle 17 #68-83), así como en los entornos de nube Azure y OCI mediante acceso remoto autorizado. Las sesiones de trabajo podrán realizarse de forma remota (priorizando la eficiencia operativa) o presencial en sitio cuando la actividad así lo requiera, previa coordinación con el supervisor del contrato, sin que ello genere costos adicionales para la entidad.

6. PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será el comprendido entre la suscripción del acta de inicio y el treinta y uno (31) de diciembre de 2026. En consecuencia, todas las obligaciones contractuales, incluyendo la implementación de las soluciones LAN, WiFi y Firewall, la activación de los licenciamientos, la prestación del soporte y la ejecución de la bolsa de horas, deberán ejecutarse dentro de dicho periodo.

La bolsa de horas corresponderá a una disponibilidad de consumo por demanda de la entidad y no a una asignación mensual fija. Su ejecución y certificación podrán realizarse máximo hasta el 10 de diciembre de 2026, con el fin de permitir el cierre administrativo, validación de soportes, facturación y trámite de pago dentro de la vigencia contractual. El pago se realizará contra horas efectivamente ejecutadas y aprobadas por la supervisión/interventoría.

Lo anterior, sin perjuicio de que la vigencia del licenciamiento y del soporte de fábrica adquirido tenga una duración de un (1) año contado a partir de su activación, la cual deberá realizarse dentro de la vigencia contractual.

Nota: Para los equipos FortiMail 3200E (seriales FE3K2ET320000001 y FE3K2ET321000004), el licenciamiento y soporte se renovarán únicamente hasta el 4 de mayo de 2027, fecha en la cual finaliza el soporte de fábrica conforme a la política EOS (End of Service) del fabricante.

Los plazos de ejecución para el presente proceso están definidos de la siguiente manera:

- **Soporte y licenciamiento de fábrica**: El soporte y licenciamiento adquiridos definidos en el presente documento tendrán una duración de un año contados a partir de la fecha de activación del licenciamiento y posterior a la firma del acta de inicio.
- **Licenciamiento**: El licenciamiento será entregado y activado por un año y comenzará a regir a partir de la activación y posterior a la firma del acta de inicio.
- **LAN**: La solución LAN adquirida y definida en el presente documento deberá ser implementada, probada y estabilizada en el plazo de ejecución contractual, de igual manera, el soporte y licenciamiento tendrán una duración de un año.
- **WiFi:** La solución WiFi adquirida y definida en el presente documento deberá ser implementada, probada y estabilizada en el plazo de ejecución contractual, de igual manera, el soporte y licenciamiento tendrán una duración de un año.
- **Firewall**: La solución de Firewall adquirida y definida en el presente documento deberá ser implementada, probada y estabilizada en el plazo de ejecución contractual, de igual manera, el soporte y licenciamiento tendrán una duración de un año.
- **Bolsa de Horas**: La bolsa de horas corresponde a servicios especializados que se ejecutarán bajo demanda, conforme a las necesidades definidas por la OTIC y dentro del plazo del contrato. Su utilización no implica dedicación permanente, y se destinará a actividades específicas de alto nivel técnico, tales como arquitectura, optimización, migraciones o atención de incidentes críticos. El pago se efectuará con periodicidad mensual previa certificación de horas ejecutadas, de conformidad con lo establecido en la sección 'Forma de pago' (numeral 19.3) de los Estudios Previos. En ningún caso la SED pagará horas no ejecutadas ni reconocerá valores por horas no autorizadas por el supervisor.

7. CÓDIGOS UNSPSC

El presente proceso se encuentra enmarcado dentro de los siguientes códigos del clasificador de bienes y servicios UNSPSC:

Tabla 9 Códigos UNSPSC

GRUPO	
(E) PRODUCTO DE USO FINAL	
SEGMENTO	
43000000	Difusión de Tecnologías de Información y Telecomunicaciones

FAMILIA	
43220000	Equipos o plataformas y accesorios de redes multimedia o de voz y datos

CLASE	
43222500	Equipos de seguridad de red

O

GRUPO	
(E) PRODUCTO DE USO FINAL	
SEGMENTO	
43000000	Difusión de Tecnologías de Información y Telecomunicaciones
FAMILIA	
43220000	Equipos o plataformas y accesorios de redes multimedia o de voz y datos
CLASE	
43222600	Equipo de servicio de red

O

GRUPO	
(F) SERVICIOS	
SEGMENTO	
81000000	Servicios Basados en Ingeniería, Investigación y Tecnología
FAMILIA	
81110000	Servicios Informáticos
CLASE	
81111800	Servicios de sistemas y administración de componentes de sistemas

O

GRUPO	
(F) SERVICIOS	
SEGMENTO	
81000000	Servicios Basados en Ingeniería, Investigación y Tecnología
FAMILIA	
81110000	Servicios Informáticos
CLASE	
81112200	Mantenimiento y soporte de software

8. SERVICIOS DE SOPORTE DEL IMPLEMENTADOR

- El Contratista deberá entregar los equipos y las licencias respectivas en el sitio indicado por la entidad en la ciudad de Bogotá DC.
- El Contratista deberá realizar Instalación, Implementación, configuración y puesta en marcha de las soluciones ofertadas.
- Todas las plataformas ofertadas deberán ser compatibles con la plataforma actual de la entidad.
- El Contratista deberá realizar la instalación y configuración de las soluciones con personal certificado en las plataformas ofertadas mínimo NSE 4 vigente o con sus equivalentes actualizados, conforme a las rutas oficiales de Fortinet, específicamente FCP – Network Security y/o FCSS – Network Security, la certificación será verificada y aprobada por la OTIC a través del supervisor del contrato o a quien este delegue.
- El Contratista deberá adjuntar certificación de fabricante que indique el nivel de certificación de los miembros del equipo de ingeniería asociado al proyecto.

- El contr deberá informar y entregar la documentación en la que se indiquen las líneas de comunicación y esquema de escalamiento para que la entidad adelante los requerimientos correspondientes al soporte de fábrica en modalidad 7X24, dentro de los tres (3) días calendario, siguientes a la firma del acta de inicio del contrato.
- El contratista deberá recibir las solicitudes de soporte vía telefónica o electrónicamente a través del sitio web en línea del contratista o mediante el correo electrónico proporcionado para tal fin.

La implementación de las plataformas ofertadas deberá contemplar:

- Planeación de cada una de las actividades, validadas en conjunto con la entidad.
- Configuración y alistamiento del software y firmware del hardware a la última versión estable aprobada por el fabricante.
- Implementación de las soluciones ofertadas de acuerdo con las mejores prácticas del fabricante, teniendo en cuenta una arquitectura de red segura.
- Pruebas de Servicio de las plataformas ofertadas.
- Puesta en Producción de las plataformas ofertadas.
- Configuración y estabilización de las plataformas ofertadas.
- Entrega de las soluciones ofertadas a satisfacción de la entidad
-

9. SERVICIOS DE SOPORTE CON FÁBRICA

La entidad requiere que el fabricante Fortinet brinde soporte telefónico y remoto en horario 7x24x365 sobre los incidentes que se llegaren a presentar sobre las soluciones de seguridad perimetral y LAN de su marca, implementadas en la infraestructura tecnológica de la SED, durante la vigencia del licenciamiento respectivo.

El soporte del fabricante estará orientado a la atención de fallas de hardware y a las soluciones de software de los equipos existentes y suministrados en el marco del presente proceso, conforme a las condiciones del licenciamiento.

El soporte del fabricante no incluye la ejecución directa de configuraciones complejas, en los términos precisados al final del presente numeral, las cuales serán cubiertas por el contratista a través de la bolsa de horas especializadas (numeral 3.5 del presente Anexo).

El contratista seleccionado no estará a cargo del servicio de soporte de fábrica, ya que este será gestionado directamente por la entidad ante el fabricante de las soluciones Fortinet, en modalidad Premium Support, sin perjuicio de las actividades a cargo del contratista a través de la bolsa de horas especializadas, conforme a la precisión contenida al final del presente numeral.

	PRODUCT SUPPORT	
	ELITE	PREMIUM
Focus Area	Technical support for product- or service-related issues	
Delivery Model	Globally distributed technical assistance centers (TAC)	
Service Delivery*		
Service Engagement	24x7 follow the sun plus enhanced response times and automated alerts	24x7 follow the sun
P1-P2 Escalations (Telephone Support)	15 minutes	1 hour
P3 Escalations (Web Support)	2 hours	Next business day
Operations Integration Points		
FortiCare Asset Portal	✓	✓
Technical Escalation (Phone and Web)	✓	✓
EEoS**	✓	
FortiCare Elite Portal	✓	
Automated Monitoring and Alerts	✓	
Security Rating Hygiene Recommendations	✓	
FortiGuard Service Updates		
Application Control, Botnet/C2, GeoIP, TrustedCert, and so on***	✓	✓

* Elite available for supported product lines only (table reflects FortiGate).
** EEoS is only available on designated Long Term Support (LTS) releases.

Precisión sobre el alcance del soporte de fábrica (FortiCare):

El soporte FortiCare del fabricante incluye asistencia en:

- Incidentes de hardware: Diagnóstico de fallas físicas, RMA y reemplazo de equipos.
- Incidentes de configuración estándar: Asistencia en troubleshooting de problemas técnicos, análisis de configuraciones, recomendaciones de cambio y resolución de tickets, conforme a los términos de servicio de Fortinet.

No se incluye en el soporte de fábrica:

- Ejecución directa de configuraciones complejas (diseño arquitectónico, implementación inicial, migraciones, integraciones personalizadas, traslados físicos de equipos).
- Actividades de estabilización avanzada, optimización post-implementación o ajustes por cambios en la arquitectura de nube.

Estas actividades serán cubiertas por el contratista a través de la bolsa de horas especializadas (numeral 3.5 del presente Anexo), bajo demanda y previa autorización del supervisor del contrato.

10. TRANSFERENCIA DE CONOCIMIENTO (No Certificada)

El **CONTRATISTA SELECCIONADO** deberá realizar una transferencia de conocimiento sobre la solución LAN adquirida por la Entidad, en cuyo temario se incluya conceptos sobre instalación, configuración, administración y solución de problemas de los equipos. Esta actividad no tendrá costos adicionales para la entidad.

La transferencia de conocimiento tendrá una duración mínima de 12 horas, distribuidas en sesiones teóricas y prácticas, y podrá realizarse de manera presencial o virtual, para un número máximo de 20 personas.

La transferencia de conocimiento se realizará durante el mes siguiente a la entrega del licenciamiento y puesta en producción de la solución adquirida por la entidad.

11. NIVEL DE CERTIFICACIÓN O MEMBRESÍA DEL PROVEEDOR

La Secretaría de Educación del Distrito requiere que los interesados en presentar oferta hagan parte del programa de Partners del fabricante y que a la fecha de presentación de las ofertas se encuentren activos en alguno de los siguientes niveles: **Advanced o Expert**.

El futuro contratista debe presentar junto con la propuesta una certificación emitida por el fabricante donde indique el nivel de certificación o membresía al que pertenecen, ya sea como Partner Advanced o Expert.

Esta certificación debe venir dirigida a la Secretaría de Educación del Distrito. La carta de nivel de certificación deberá estar expedida dentro de los 30 días calendario previos a la fecha de presentación de ofertas.

12. CERTIFICACIÓN DE LA CASA MATRIZ, AUTORIZACIÓN DE COMERCIALIZACIÓN

La Secretaría de Educación del Distrito exige que el proponente acredite que se encuentra autorizado por

el fabricante (Fortinet) para ofrecer, distribuir y comercializar los productos objeto del presente proceso. Dicha autorización deberá demostrarse mediante la presentación de una (1) certificación vigente, expedida por el fabricante o por su representante legal en Colombia, dirigida al proponente.

Esta certificación acredita la calidad de Partner Autorizado y NO está asociada a la cantidad de licencias o equipos ofertados; un solo documento es suficiente para cumplir con el requisito, independientemente del número de ítems incluidos en la propuesta.

Esta certificación debe venir dirigida a la Secretaría de Educación del Distrito. La carta de nivel de certificación deberá estar expedida dentro de los 30 días calendario previos a la fecha de presentación de ofertas.

En caso de que la documentación sea presentada por un proponente plural, el requisito se entenderá cumplido cuando alguno de los integrantes presente la certificación en los términos aquí solicitados.

13. ACUERDOS DE CONFIDENCIALIDAD

Toda la información a la que tenga acceso el **CONTRATISTA SELECCIONADO**, así como los informes, documentos, registros, configuraciones y demás entregables que se generen con ocasión de la ejecución 3del contrato, será considerada **información confidencial** de propiedad de la **Secretaría de Educación del Distrito (SED)**.

En consecuencia, el CONTRATISTA SELECCIONADO se obliga a **proteger la confidencialidad, integridad y disponibilidad** de la información institucional, comprometiéndose a no divulgarla, reproducirla, transferirla, modificarla o utilizarla para fines distintos a los estrictamente relacionados con el objeto contractual, sin la **autorización previa, expresa y por escrito** de la SED.

El acceso a la información, a los activos tecnológicos y a los servicios de procesamiento de información de la SED estará condicionado a la **aceptación y firma previa de los acuerdos de confidencialidad**, los cuales deberán ser formalizados al inicio del contrato y mantenerse vigentes durante toda su ejecución, y con posterioridad a su terminación, conforme a la normativa aplicable.

El CONTRATISTA SELECCIONADO será responsable de adoptar las **medidas técnicas, administrativas y organizacionales necesarias** para prevenir accesos no autorizados, alteraciones indebidas, pérdida, destrucción o indisponibilidad de la información, de acuerdo con las políticas de seguridad de la información de la SED y los lineamientos del Estado colombiano.

ASPECTO	NOMBRE	Firma/VoBo
Aprobó:	MILENA DEL PILAR SANDOVAL GOMEZ - Jefe Oficina de las Tecnologías de la Información	
Elaboró aspectos técnicos	Juan Carlos Parra M. – Oficial Seguridad Informática OTIC	
Elaboró aspectos Jurídicos	José Esteban Bueno Rivero – Profesional Contratista OTIC	
Revisó aspectos técnicos	Carlos Alberto López Díaz – Profesional Contratista OTIC	
Revisó aspectos técnicos	Omar Ardila Torres– Profesional Contratista OTIC	
Revisó aspectos técnicos	Jorge Iván Vergara Sornoza – Profesional Contratista OTIC	
Revisó aspectos técnicos	Jairo Alberto Orduz Salamanca – Profesional Especializado OTIC	