MINISTERIO DE DEFENSA NACIONAL **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR**	**CONTRATO DE COMPRAVENTA No.:**	**043-2020 DEJPM-MDN**
	CONTRATANTE:	**DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MINISTERIO DE DEFENSA NACIONAL**
	NIT:	900.384.997-1
	CONTRATISTA:	**USCOM S.A.S.**
	NIT:	900.396.229-3
	OBJETO:	Adquisición de equipos de seguridad perimetral firewall para la Dirección Ejecutiva de la Justicia Penal Militar - MDN incluido licenciamiento, soporte en sitio requerido y mantenimiento de conformidad con las especificaciones técnicas mínimas exigidas; hacen parte integral del mismo los Anexos 1,2 y 3.
	PLAZO:	El plazo de ejecución del contrato será hasta el 31 de diciembre de 2020, contados a partir del perfeccionamiento del contrato, previa presentación de la planilla donde conste el pago por parte de **USCOM S.A.S.**, de los aportes parafiscales y a la seguridad social integral del mes anterior, expedición del registro presupuestal por parte de la entidad y aprobación de la garantía única de cumplimiento y de responsabilidad civil y extracontractual.
	VALOR:	**TRESCIENTOS CINCUENTA Y CINCO MILLONES CUATROCIENTOS SESENTA Y TRES MIL NOVECIENTOS NOVENTA Y DOS PESOS CON OCHENTA CENTAVOS M/CTE. ($355.463.992,80)**, incluido IVA y demás erogaciones a que haya lugar.

Bogotá D.C., 16 DIC. 2020

Entre los suscritos **FABIO ESPITIA GARZÓN**, mayor de edad, identificado con cédula de ciudadanía No. 79.254.557, en su calidad de **DIRECTOR EJECUTIVO DE LA JUSTICIA PENAL MILITAR**, designado mediante Resolución Ministerial No. 2105 de 21 de julio de 2020 y Acta de Posesión No. 0066-20 del 27 de julio de

2020, debidamente facultado para celebrar contratos de conformidad con lo dispuesto en la Resolución Ministerial No. 4519 de 27 de mayo de 2016, modificada parcialmente por la Resolución Ministerial No. 1417 del 08 de marzo de 2018, quien representa a la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN**, con **NIT 900.384.997-1**, por una parte, y por la otra el señor **OTTO FRANCISCO URREA JARAMILLO**, mayor de edad, identificado con cédula de ciudadanía No. 79.695.683 de Bogotá D.C., quien actúa en representación de la empresa **USCOM S.A.S.,** con NIT. 900.396.229-3, según Certificado de Existencia y Representación Legal expedido por la Cámara de Comercio de Bogotá y quien para los efectos de este documento se denominará **EL CONTRATISTA**, hemos convenido celebrar el presente contrato de compraventa, previa las siguientes consideraciones: **1)** Que conforme a lo establecido en la Ley 80 de 1993, la Ley 1150 de 2007, la Ley 1474 de 2011 y el artículo 2.2.1.2.1.2.20 del Decreto Único Reglamentario 1082 de 2015, la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** adelantó el proceso de Selección Abreviada – Subasta Inversa Electrónica No. 043-2020 DEJPM-MDN, cuyo objeto es: "*Adquisición de equipos de seguridad perimetral firewall para la Dirección Ejecutiva de la Justicia Penal Militar - MDN incluido licenciamiento, soporte en sitio requerido y mantenimiento de conformidad con las especificaciones técnicas mínimas exigidas*". **2)** Que en los Estudios Previos se estableció con claridad y precisión la necesidad a contratar, los aspectos técnicos del objeto, el valor estimado del contrato, la modalidad de contratación y demás elementos que deben contener los estudios previos, dando cumplimiento a lo establecido en los numerales 7° y 12 del artículo 25 de la Ley 80 de 1993 y del Decreto Único Reglamentario 1082 de 2015. **3)** Que frente a la necesidad presentada se han analizado las alternativas de solución y se ha llegado a la conclusión que lo más conveniente es la "*Adquisición de equipos de seguridad perimetral firewall para la Dirección Ejecutiva de la Justicia Penal Militar - MDN incluido licenciamiento, soporte en sitio requerido y mantenimiento de conformidad con las especificaciones técnicas mínimas exigidas*". **4)** Que mediante Resolución No. 000262 del 24 de noviembre de 2020, se ordenó la apertura del Proceso de Selección Abreviada – Subasta Inversa Electrónica No. 043-2020 DEJPM-MDN, contando con la respectiva apropiación presupuestal. **5)** Que en cumplimiento con lo ordenado por el Decreto Único Reglamentario 1082 de 2015, se dio publicidad al Proyecto de Pliego de Condiciones y al Pliego de Condiciones Definitivo en la plataforma del Portal Colombia Compra Eficiente - Sistema Electrónico de la Contratación Pública–SECOP II www.colombiacompra.gov.co. **6)** Que el 30 de noviembre de 2020, a las diez (10:00) horas, conforme a lo señalado en el cronograma del proceso publicado en la plataforma del Portal Colombia Compra Eficiente - Sistema Electrónico de la Contratación Pública – SECOP II www.colombiacompra.gov.co se cerró la convocatoria del proceso de Selección Abreviada Subasta Inversa No. 043-2020 DEJPM-MDN, presentándose propuestas por parte de las empresas: USCOM S.A.S., SOFTSECURITY S.A.S., S3 SIMPLE SMART SPEEDY S.A., IT SERVICIOS DE COLOMBIA S.A.S. y GAMMA INGENIEROS S.A.S. **7)** Que realizada la verificación de los requisitos habilitantes de las condiciones jurídicas, técnicas, financieras y organizacionales de las ofertas presentadas, la Dirección Ejecutiva de la Justicia Penal Militar - MDN efectuó traslado del informe preliminar de evaluación de las ofertas, debidamente

publicado en el Portal Colombia Compra Eficiente – Sistema Electrónico de la Contratación Pública – SECOP II www.colombiacompra.gov.co, por el término de tres (3) días hábiles, esto es, del 3 al 7 de diciembre de 2020, hasta las 23:00 horas. **8)** Que durante el término de traslado del informe de evaluación preliminar se allegaron subsanaciones de los documentos habilitantes y se presentaron observaciones por parte de IT SERVICIOS DE COLOMBIA S.A.S., siendo estas resueltas mediante "*CUADERNILLO DE PREGUNTAS Y RESPUESTAS No. 1 A LAS OBSERVACIONES PRESENTADAS AL INFORME DE EVALUACIÓN PRELIMINAR DEL PROCESO DE SELECCIÓN ABREVIADA SUBASTA INVERSA No. 043-2020 DEJPM-MDN*", publicado en el Portal de Colombia Compra Eficiente - Sistema Electrónico de la Contratación Pública - SECOP www.colombiacompra.gov.co. **9)** Que mediante "*CUADERNILLO DE PREGUNTAS Y RESPUESTAS No. 2 A LAS OBSERVACIONES EXTEMPORANEAS PRESENTADAS A LA AL INFORME DE EVALUACION DEFINITIVO DEL PROCESO DE SELECCIÓN ABREVIADA SUBASTA INVERSA No. 043-2020 DEJPM-MDN*" publicado en el Portal de Colombia Compra Eficiente - Sistema Electrónico de la Contratación Pública - SECOP www.colombiacompra.gov.co., el 12 de diciembre de 2020, se dio respuesta a las observaciones extemporáneas presentadas por SOFTSECURITY y S3 SIMPLE SMART SPEEDY S.A.S., al informe definitivo de evaluación técnica. **10**) Que mediante Resolución No. 000282 del 14 de diciembre de 2020, se adjudicó Proceso de Selección Abreviada – Subasta Inversa Electrónica No. 043-2020 DEJPM-MDN a la empresa **USCOM S.A.S.**, por cumplir con los requerimientos técnicos, jurídicos, económicos – financieros y organizacionales exigidos, por ajustarse al presupuesto oficial asignado para el proceso y de acuerdo con la recomendación del Comité de Adquisiciones consignada en el Acta No. 65 de 14 de diciembre de 2020. **11)** Que habiéndose dado cumplimiento a los trámites y requisitos legales que exige el Estatuto General de Contratación de la Administración Pública, es procedente la celebración del presente Contrato de Compraventa, el cual se regirá por las siguientes cláusulas: **CLÁUSULA PRIMERA - OBJETO:** Adquisición de equipos de seguridad perimetral firewall para la Dirección Ejecutiva de la Justicia Penal Militar - MDN incluido licenciamiento, soporte en sitio requerido y mantenimiento de conformidad con las especificaciones técnicas mínimas exigidas; hacen parte integral del mismo los Anexos 1,2 y 3. **CLÁUSULA SEGUNDA - ALCANCE DEL OBJETO:** En desarrollo del objeto **USCOM S.A.S.**, deberá suministrar, configurar, instalar y poner en funcionamiento los equipos de seguridad perimetral firewall para la Dirección Ejecutiva de la Justicia Penal Militar – MDN, incluido licenciamiento, soporte y mantenimiento de conformidad con las especificaciones técnicas previstas en el Anexo No. 1 "***ANEXO TÉCNICO DEL CONTRATO***", el cual se suscribe por parte de **USCOM S.A.S.,** y hace parte integral del presente contrato. **CLÁUSULA TERCERA - VALOR:** Para efectos fiscales y presupuestales, el valor del presente contrato es por la suma de **TRESCIENTOS CINCUENTA Y CINCO MILLONES CUATROCIENTOS SESENTA Y TRES MIL NOVECIENTOS NOVENTA Y DOS PESOS CON OCHENTA CENTAVOS M/CTE. (355.463.992,80)**, incluido IVA y demás erogaciones a que haya lugar, distribuidos así:

ITEM	NOMBRE	CANTIDAD FINAL	PRESENTACIÓN REQUERIDA	VALOR TOTAL IVA INLCUIDO
1	**HARDWARE**			
1.1	FIREWALLS NEXT GENERATION, CON GARANTÍA MINIMA DE UN AÑO, INCLUIDO LOS ACCESORIOS NECESARIOS PARA EL HA.	2	Unidad	$134.843.247,00
1.2	DOS (2) UNIDADES DE MÓDULOS SFP+ 1GB Y DOS (2) UNIDADES SFP+ 10GB, POR CADA EQUIPO QUE HAGA PARTE DEL CLUSTER, INCLUIDO CABLES DE CONEXIÒN.	8	Unidad	$ 9.361.018,80
2.	**LICENCIAMIENTO POR UN (1 AÑO) DEL FIREWALL.**			
2.1	LICENCIAMIENTO CONTROL DE APLICACIONES.	2	Unidad	$35.740.624,50
2.2	LICENCIAMIENTO PREVENCIÓN DE AMENAZAS – IPS PRÓXIMA GENERACIÓN, ANTIVIRUS DE RED, ANTISPYWARE	2	Unidad	$18.785.718,00
2.3	LICENCIAMIENTO FILTRADO WEB.	2	Unidad	$21.173.733,00
2.4	LICENCIAMIENTO PREVENCIÓN AMENAZAS DÍA CERO	2	Unidad	$29.452.185,00
3.	**SERVICIOS DE MANTENIMIENTO, GESTIÓN, SOPORTE, BOLSA DE HORAS.**			
3.1	MIGRACIÓN DE LA PLATAFORMA ACTUAL, MARCA CHECKPOINT, COMPRENDIDA POR LOS SIGUIENTES ELEMENTOS: • DOS (02) FIREWALL NGFW 4800 VERSIÓN R77.30 • UN (01) MANAGEMENT VIRTUAL OPEN SERVER VERSIÓN R80.20 • UN (01) EVENTIA REPORT VIRTUAL OPEN SERVER VERSIÓN R80.20 A LA NUEVA SOLUCIÓN OFERTADA.	1	Unidad	$30.884.994,00
3.2	SOPORTE A INCIDENTES DE 1° Y 2° NIVEL EN MODALIDAD 7X24 PARA LOS DOS (2) FIREWALL POR UN AÑO DIRECTAMENTE DEL FABRICANTE.	1	Unidad	$37.014.232,50
3.3	BOLSA DE 192 HORAS DE ASISTENCIA EN SITIO Y/O REMOTO PARA LA ADMINISTRACIÓN DE LA SOLUCIÓN.	192	HORAS	$38.208.240,00

PARÁGRAFO PRIMERO: Los valores ofertados por **USCOM S.A.S.,** a través de la plataforma del SECOP II, se entenderán firmes y fijos, por lo tanto, no están sujeto a ninguna clase de reajuste. Igualmente, dentro de estos precios están incluidos los costos proyectados al plazo de ejecución del presente contrato y la utilidad razonable que **USCOM S.A.S.** pretende obtener, en consecuencia, no se aceptarán solicitudes de reajuste fundamentados en estas circunstancias. **PARÁGRAFO SEGUNDO:** La **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN,** efectuará en el Certificado de Registro Presupuestal la liberación del valor que no llegare a ser ejecutado en la respectiva vigencia si a ello hubiera lugar, previa solicitud del supervisor del contrato. Lo anterior se verá reflejado en el acta de liquidación correspondiente. **CLÁUSULA TERCERA - FORMA DE PAGO:** La **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** pagará el valor del contrato a **USCOM S.A.S.,** es decir, la suma de **TRESCIENTOS CINCUENTA Y CINCO MILLONES CUATROCIENTOS SESENTA Y TRES MIL**

NOVECIENTOS NOVENTA Y DOS PESOS CON OCHENTA CENTAVOS M/CTE. ($355.463.992,80), así: **a)** Un pago por la suma de **CIENTO CUARENTA Y CUATRO MILLONES DOSCIENTOS CUATRO MIL DOSCIENTOS SESENTA Y CINCO PESOS CON OCHENTA CENTAVOS M/CTE. ($144.204.265,80)**, por concepto de la entrega de los equipos que hacen parte del hardware, por parte de **USCOM S.A.S.**, previa suscripción del acta de recibo a satisfacción de los equipos y presentación del anexo contractual de catalogación. **b)** Un pago por la suma de **CIENTO CINCO MILLONES CIENTO CINCUENTA Y DOS MIL DOSCIENTOS SESENTA PESOS CON CINCUENTA CENTAVOS M/CTE. ($105.152.260,50)**, por concepto de la entrega de las licencias por parte de **USCOM S.A.S.**, previa suscripción del acta de recibo a satisfacción de las licencias y presentación del anexo contractual de catalogación. **c)** Un pago por la suma de **CIENTO SEIS MILLONES CIENTO SIETE MIL CUATROCIENTOS SESENTA Y SEIS PESOS CON CINCUENTA CENTAVOS M/CTE. ($106.107.466,50)** por concepto de los servicios de migración de la plataforma, soporte de asistencia técnica y servicio de bolsa de horas conforme al consumo ejecutado. Los pagos de los literales **a**), **b**), y **c**) se realizarán dentro de los sesenta (60) días calendarios siguientes a la fecha de expedición del certificado de cumplimiento a satisfacción por parte del supervisor del contrato, previa presentación de las facturas, así como la verificación del pago al sistema de seguridad social, aportes parafiscales y dando cumplimiento a los demás trámites administrativos a que haya lugar, la presentación de la factura no podrá ser posterior al 24 de diciembre de 2020, con el objeto de configurarse la respectiva cuenta por pagar y cumplimiento de los demás trámites administrativos a que hay lugar. **PARÁGRAFO PRIMERO**: La **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** pagará el valor total del contrato a **USCOM S.A.S.**, en moneda legal colombiana, a través de la Tesorería del Grupo Logístico Administrativo y Financiero, una vez se encuentre aprobado el PAC (Programa Anual Mensualizado de Caja), mediante consignación en la cuenta que **USCOM S.A.S.**, acredite como propia. **PARÁGRAFO SEGUNDO:** En el valor del contrato se entiende incluido IVA y demás erogaciones a que haya lugar. El porcentaje por concepto del impuesto al valor agregado IVA se calculará, de conformidad con las disposiciones que rijan la materia. Todos los pagos efectuados tendrán los descuentos de ley. **PARÁGRAFO TERCERO**: Para la realización de los pagos derivados del presente contrato, **USCOM S.A.S.**, deberá entregar al supervisor la CONSTANCIA DEL PAGO DE APORTES AL SISTEMA DE SEGURIDAD SOCIAL INTEGRAL (SALUD, PENSIÓN Y RIESGOS LABORALES), y APORTES PARAFISCALES, de acuerdo con el artículo 50 de la Ley 789 de 2002, modificado por la Ley 828 de 2003, de sus trabajadores y de sus contratistas, mediante certificación expedida por el revisor fiscal, junto con la última planilla donde se evidencie el pago realizado, exonerándose del mismo para aquellos casos que se encuentran contemplados en el artículo 25 de la Ley 1607 de 2012. La certificación emitida por parte del revisor fiscal deberá acompañarse de la copia de la tarjeta profesional, la cédula de ciudadanía y el certificado de la Junta Central de Contadores con una fecha de emisión no mayor a noventa (90) días calendario. **PARÁGRAFO CUARTO – CUENTA PARA PAGO:** El pago previsto se realizará en la cuenta corriente No. 540014222 del Banco BBVA COLOMBIA, según certificación bancaria expedida el 20 de noviembre de 2020, donde se señaló como

titular de la misma a **USCOM S.A.S.**, o en otra cuenta bancaria de la que sea titular **USCOM S.A.S.**, y lo informe por escrito a la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** con no cinco (5) días de anticipación a la presentación de la factura enviando la respectiva certificación bancaria en donde se acredite su apertura y titularidad. **PARÁGRAFO QUINTO**: Si la factura no ha sido correctamente elaborada o no se acompaña de los documentos requeridos en original para el pago y/o se presentan de manera incorrecta, el término para éste sólo empezará a contarse desde la fecha en que se aporte en debida forma o se allegue el último de los documentos y aplicará la misma regla de trámite en el mes siguiente a la presentación si la corrección no se hace dentro de los primeros cinco (5) días hábiles siguientes. Las demoras que se presenten por estos conceptos, serán responsabilidad de **USCOM S.A.S.**, y no tendrán por ello derecho al pago de intereses o compensación de ninguna naturaleza. **PARÁGRAFO SEXTO. – REAJUSTE AL PESO: USCOM S.A.S.**, acepta que en el evento que el valor total a pagar tenga centavos, estos se ajusten o aproximen al peso, ya sea por exceso o por defecto, si la suma es mayor o menor a 50 centavos. Lo anterior, sin que sobrepase el valor total establecido en el presente contrato. **CLÁUSULA CUARTA - APROPIACIÓN PRESUPUESTAL:** El valor que la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** se compromete a pagar a **USCOM S.A.S.,** como contraprestación por el cumplimiento del objeto contratado, se encuentra soportado Certificado de Disponibilidad Presupuestal No. 10920 del 23 de julio de 2020, reducido el 15 de octubre y adicionado el 16 octubre del año en curso, con rubro presupuestal A-02-01-01-004-005 MAQUINARIA DE OFICINA, CONTABILIDAD E INFORMÁTICA, A-02-01-01-006-002 PRODUCTOS DE LA PROPIEDAD INTELECTUAL y A-02-02-02-008-007 SERVICIOS DE MANTENIMIENTO REPARACION E INSTALACION (EXCEPTO SERVICIOS DE CONSTRUCCION) respaldado en el Certificado Plan Anual de Adquisiciones No. 28 MDN-DEJPM-GLAF 40.63 del 23 de julio de 2020, modificado el 16 de octubre del mismo año, expedidos por el Grupo Logístico Administrativo y Financiero de la Dirección Ejecutiva de la Justicia Penal Militar – MDN. **CLÁUSULA QUINTA - PLAZO DE EJECUCIÓN:** El plazo de ejecución del contrato será hasta el 31 de diciembre de 2020, contados a partir del perfeccionamiento del contrato, previa presentación de la planilla donde conste el pago por parte de **USCOM S.A.S.**, de los aportes parafiscales y a la seguridad social integral del mes anterior, expedición del registro presupuestal por parte de la entidad y aprobación de la garantía única de cumplimiento y de responsabilidad civil extracontractual. **CLÁUSULA SEXTA - VIGENCIA DEL CONTRATO:** La vigencia del presente contrato comprende el plazo de ejecución y cuatro (4) meses más. **CLÁUSULA SÉPTIMA - LUGAR DE EJCUCIÓN:** El lugar de ejecución del contrato será en el Edificio Palacio de Justicia Penal Militar y Policial "TF. Laura Rocío Prieto Forero", ubicado en el Cantón Militar Caldas en la Carrera 46 No. 20C-1 de la ciudad de Bogotá D.C. **CLÁUSULA OCTAVA - DERECHOS DE USCOM S.A.S.:** En general, son derechos de **USCOM S.A.S.: 1)** Recibir el pago en la forma y oportunidad establecida en el presente contrato. **2)** Tener acceso a los elementos físicos necesarios para desarrollar el objeto y cumplir con sus obligaciones. **3)** Celebrar todos los contratos y operaciones que considere útiles a sus intereses, siempre que se encuentren dentro del ámbito de los derechos y obligaciones que surgen con ocasión del presente contrato y que

sean consistentes con su finalidad. **4)** Obtener la colaboración necesaria de la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MDN** para el adecuado desarrollo del contrato. **CLÁUSULA NOVENA - OBLIGACIONES DE USCOM S.A.S.:** En general son obligaciones de **USCOM S.A.S.: 1.** Cumplir con el objeto del contrato en los términos establecidos en los estudios y documentos previos, en el pliego de condiciones, sus adendas si fueran expedidas, el anexo de especificaciones técnicas mínimas exigidas y en la oferta presentada, lo cual para todos los efectos forma parte integral del contrato. **2**. Ofrecer un (1) año de garantía y soporte prestado directamente por el fabricante, tanto para el software y hardware, contado a partir del recibo a satisfacción de la Entidad. **3**. **USCOM S.A.S.**, realizará las gestiones necesarias para la visualización del licenciamiento señalado en las especificaciones técnicas mínimas exigidas a través del portal web del fabricante, dentro los quince (15) días calendario siguiente a la legalización del contrato. **4**. En caso de presentarse fallas en los sistemas de seguridad Firewall **USCOM S.A.S.**, deberá efectuar los mantenimientos correctivos que se requieran y las veces que sea necesario; sin que ello genere costo adicional al valor total del contrato. **5**. **USCOM S.A.S.**, garantizará que las actividades desarrolladas durante la ejecución del contrato no interfieran en la continuidad, disponibilidad, integridad e interoperabilidad de los servicios informáticos de la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN. 6**. **USCOM S.A.S.**, deberá realizar las gestiones necesarias para garantizar el óptimo y correcto funcionamiento del sistema Firewall y mantener actualizados cada uno de los componentes del mismo. Para esto, deberá implementar durante la ejecución del contrato y la vigencia del mismo, las actualizaciones liberadas por el fabricante y prestar soporte de fábrica y capacitar a la Entidad sobre cada una de ellas, sin que esto genere costos o erogaciones adicionales para la Entidad. **7**. **USCOM S.A.S.**, garantizará que el servicio de soporte en sitio y/o remoto, acompañamiento en la operación y mantenimiento del Firewall se realice por personal idóneo de conformidad con lo establecido en las especificaciones técnicas mínimas exigidas. **8**. En caso que durante la ejecución del contrato sea necesario el cambio de alguno de los perfiles solicitados en las especificaciones técnicas **USCOM S.A.S.**, deberá informar por escrito al supervisor del contrato inmediatamente a la ocurrencia del hecho y deberá garantizar el reemplazo del mismo a más tardar dentro de los tres (03) días hábiles siguientes al aviso con personal de igual o superior perfil, adjuntando la correspondiente documentación. **9**. **USCOM S.A.S.**, deberá entregar al supervisor designado por parte de la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** la información solicitada en el Anexo *"CLÁUSULA CONTRACTUAL DE CATALOGACIÓN"*, dentro de los cinco (5) hábiles posteriores a la aprobación de la póliza de cumplimiento y de responsabilidad civil extracontractual, que garantice las obligaciones del contrato. **10**. Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones que puedan presentarse y, en general, se obliga a cumplir con lo establecido en la Ley 80 de 1993, la Ley 1150 de 2007 y sus decretos reglamentarios. **11**. Atender las indicaciones y recomendaciones que le imparta el funcionario señalado por la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** como supervisor del contrato. **12**. Asistir a las reuniones programadas por el supervisor del contrato que la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR –**

MDN designe. **13**. Responder sin perjuicio de la respectiva garantía, por la calidad del servicio y/o de los bienes suministrados. **14**. **USCOM S.A.S.**, deberá cumplir con la normatividad vigente en pro de la seguridad y salud de sus trabajadores, de conformidad con lo exigido en el Decreto Único Reglamentario 1072 de 2015, libro 2, titulo 4, capítulo 6, Sistema de Gestión de la Seguridad y Salud en el Trabajo, que le permitan a **USCOM S.A.S.**, anticipar, reconocer, evaluar y controlar los riesgos que puedan afectar la seguridad y salud en el trabajo. **15**. Allegar dentro de los tres (3) días siguientes al perfeccionamiento del contrato el certificado de curso virtual de cincuenta (50) horas sobre Seguridad y Salud en el Trabajo (Artículo 2.2.4.6.35 del Decreto Único Reglamentario 1072 de 2015) y mantenerlo vigente. **16**. El personal que prestará los servicios en las instalaciones de la de la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN**, deberá contar con todos los elementos de bioseguridad establecidos en el protocolo determinado por la Entidad. **17**. Mantener la debida reserva frente a los temas y asuntos tratados y conocidos dentro del desarrollo y ejecución del contrato, de conformidad con el compromiso de confidencialidad que se suscribe con el contrato y que hace parte integral del mismo. **18**. Cumplir cabalmente con sus obligaciones frente al Sistema de Seguridad Social Integral (Salud, Pensión y Riesgos Laborales) y Aportes Parafiscales (Cajas de Compensación Familiar, SENA e ICBF). Para la realización del pago derivado del contrato **USCOM S.A.S.**, deberá entregar al supervisor certificación expedida por el revisor fiscal en la que acredite que se encuentra al día en el pago de las citadas obligaciones, exonerándose del mismo para aquellos casos que se encuentran contemplados en el artículo 25 de Ley 1607 de 26 de diciembre de 2012; también deberá adjuntar las últimas dos (2) planillas en donde conste estar al día con este pago. **19**. Constituir en debida forma y aportar a la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MDN**, la garantía única de cumplimiento y de responsabilidad civil extracontractual dentro del término señalado para el efecto en el cronograma del proceso. **20**. **USCOM S.A.S.**, mantendrá indemne a la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MDN** contra todo reclamo, demanda, acción legal, y costos que puedan causarse o surgir por daños o lesiones a personas o bienes, ocasionados por **USCOM S.A.S.**, o su personal, durante la ejecución del objeto y obligaciones del contrato. **21**. En general, la obligación de cumplir cabalmente con las condiciones y modalidades previstas contractualmente para la ejecución y desarrollo del contrato, para lo cual **USCOM S.A.S.**, deberá actuar razonablemente en el marco de sus obligaciones contractuales. **22**. Cumplir con los descuentos valores otorgados en la subasta, la cual forma parte integrante del presente contrato y se mantendrá vigente durante el tiempo de ejecución del mismo. **23**. Las demás obligaciones que sean necesarias para la adecuada ejecución del objeto contractual. **CLÁUSULA DÉCIMA - DERECHOS DE LA DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MDN**: **1)** Supervisar el desarrollo y ejecución del presente contrato, y acceder a los documentos e información que soportan la labor de **USCOM S.A.S. 2)** Solicitar y recibir información técnica respecto de los bienes y/o servicios, y demás elementos que suministre **USCOM S.A.S.,** en desarrollo del objeto del presente contrato. **3)** Rechazar los servicios prestados y/o bienes suministrados cuando no cumplan con las especificaciones técnicas exigidas descritas en el Anexo No. 1 "***ANEXO TÉCNICO DEL CONTRATO***". **4)**

Mantener comunicación permanente y directa con el interlocutor designado por **USCOM S.A.S.,** a través del supervisor designado por la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN. CLÁUSULA DÉCIMA PRIMERA - OBLIGACIONES DE LA DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MDN: 1)** Poner a disposición de **USCOM S.A.S.**, los bienes y lugares que se requieran para la ejecución del objeto contratado. **2)** Recibir a satisfacción los bienes y/o servicios prestados que sean entregados por **USCOM S.A.S.**, cuando estos cumplan con las condiciones establecidas en el presente contrato y, en especial, las especificaciones técnicas contenidas en el Anexo No. 1 "***ANEXO TÉCNICO DEL CONTRATO***" del presente contrato. **3)** Pagar a **USCOM S.A.S.**, el valor del contrato en la forma, con sujeción a las apropiaciones presupuestales y disponibilidad de PAC, prevista para el efecto. **4)** Designar un supervisor para el presente contrato, el cual representará a la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** ante **USCOM S.A.S.**, para supervisar y certificar el cumplimiento del objeto del contrato. **5)** Tomar las decisiones necesarias para la correcta ejecución del objeto contractual. **CLÁUSULA DÉCIMA SEGUNDA - SUPERVISIÓN:** De conformidad con lo señalado en la Resolución No. 000233 de 30 de octubre de 2020, el supervisor del presente contrato será el **PD. FREDY ARBEY ROMERO SILVA**, con el fin de vigilar permanentemente la correcta ejecución del objeto contratado, de conformidad con lo establecido en el artículo 83 de la Ley 1474 de 2011, que señala quien ejercerá las actividades de supervisión y control de la ejecución del contrato que le corresponde directamente, de conformidad con lo establecido en el artículo 26 de la Ley 80 de 1993, en el artículo 84 de la Ley 1474 de 2011, en la Resolución Ministerial No. 6302 de 2014 numeral 5.3.1.7 "*DE LA SUPERVISIÓN O INTERVENTORÍA DE LOS CONTRATOS*" y siguientes, en concordancia con la Directiva Permanente No. 12 del 21 de septiembre de 2020, y tendrá las siguientes obligaciones: **a.** Suministrar toda la información normativa y técnica disponible para la ejecución del contrato. **b.** Supervisar técnica, administrativa y legalmente la ejecución del contrato. **c.** Exigir a **USCOM S.A.S.**, la información que considere necesaria para verificar la correcta ejecución del contrato y para ejercer de manera general el control del mismo. **d.** Exigir el cumplimiento del contrato en todas y cada una de sus partes. **e.** Verificar directamente que **USCOM S.A.S.**, cumpla con las condiciones de ejecución del contrato según los términos pactados, para lo cual tendrá la facultad de requerirlo por escrito, con el fin de que corrija el incumplimiento en el que esté incurriendo o pueda incurrir. **f.** Verificar y dejar constancia del cumplimiento de las obligaciones del Sistema de Seguridad Social Integral y Parafiscales, de conformidad con lo establecido en el artículo 50 de la Ley 789 de 2002, y en el artículo 23 de la Ley 1150 de 2007, exonerándose del mismo para aquellos casos que se encuentran contemplados en el artículo 25 de Ley 1607 del 26 de diciembre de 2012. En caso contrario deberá dar aviso de esta circunstancia al Grupo de Asesoría Legal de la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN. g.** Cualquier modificación que se deba realizar al plazo de ejecución del contrato debe ser previamente autorizada por el competente contractual. **h.** El supervisor deberá resolver todas las consultas presentadas por **USCOM S.A.S.**, y hacerle las observaciones que estime convenientes. Si durante la ejecución del contrato se presentan dudas o diferencias que no puedan ser resueltas por el supervisor, éste

deberá remitirlas mediante oficio, dentro de los tres (3) días hábiles siguientes a la ocurrencia de las mismas, al competente contractual para su consulta y decisión, con copia al Grupo de Asesoría Legal de la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN. i.** Expedir el certificado de cumplimiento a **USCOM S.A.S.**, respecto de las obligaciones objeto del presente contrato, previa entrega de la factura por parte del mismo (si a ello hubiere lugar), en donde conste claramente el nombre y firma de la persona que lo recibió y copia del documento que acredite el pago por parte de **USCOM S.A.S.**, al Sistema de Seguridad Social Integral y/o Aportes Parafiscales, según corresponda. La documentación anterior deberá remitirla al Grupo Logístico Administrativo y Financiero de la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** para el trámite de pago correspondiente. **j.** Informar al Grupo de Asesoría Legal de la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** cualquier demora o incumplimiento en las obligaciones por parte de **USCOM S.A.S.**, dentro de los cinco (5) días siguientes a la ocurrencia del hecho, de conformidad con los plazos señalados en las especificaciones técnicas mínimas exigidas. **k.** Elaborar informes sobre el avance y ejecución del contrato, de conformidad con lo establecido en la Resolución Ministerial No. 6302 del 31 de julio de 2014, "*Por la cual se Adopta el Manual de Contratación del Ministerio de Defensa Nacional, y sus Unidades Ejecutoras*". **l.** El supervisor deberá constatar a la fecha de vencimiento del contrato su total cumplimiento. Si llegare a tener observaciones o inquietudes sobre la ejecución del mismo, no podrá expedir el certificado de cumplimiento final hasta tanto no sean clarificadas. **m.** Elaborar a la terminación del contrato, de conformidad con lo señalado en la cláusula del presente contrato que establezca el acta de liquidación, la cual deberá remitirse al Grupo Asesoría Legal de la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN**, para su revisión y aceptación, y proceder al trámite de suscripción de la misma. La obligación aquí establecida sólo se entenderá cumplida por el supervisor una vez se encuentre suscrita el acta final de liquidación por **USCOM S.A.S.**, y el competente contractual. **n.** El supervisor debe, si es necesario, solicitar la suspensión temporal de la ejecución del contrato por circunstancias de fuerza mayor o caso fortuito, justificando plenamente las circunstancias de modo, tiempo y lugar que originan los hechos de la suspensión, ante el competente contractual, mediante documento escrito, para que éste emita su autorización. **o.** Realizar constancia de cierre del expediente del proceso en los términos de lo establecido en el artículo 2.2.1.1.2.4.3 del Decreto Único Reglamentario 1082 de 2015. **p.** Solicitar, si llegare a ser necesario, la suspensión temporal de la ejecución del contrato por circunstancia de fuerza mayor o caso fortuito, justificando plenamente las circunstancias de tiempo, modo y lugar que originan los hechos de la suspensión, ante el competente contractual mediante documento escrito, para que éste emita su autorización. **q.** El supervisor deberá allegar al expediente contractual, el informe de ejecución (cuando aplique), junto con el cumplido a satisfacción, la factura (si aplica) y los demás documentos exigidos para cada pago. Para efectos del trámite respectivo al Grupo Logístico Administrativo y Financiero y al Grupo de Asesoría Legal, para la respectiva publicación en la plataforma del SECOP II. **r.** El supervisor del contrato deberá de conformidad con el artículo 2.2.1.1.2.4.3 del Decreto 1082 de 2015, hacer seguimiento al cumplimiento y

efectividad de las garantías según corresponda y dentro delos términos contractuales y legales. Así mismo, realzará el cierre del expediente contractual, dejando constancia del cumplimiento del contrato y del uso o no de las garantías. Es importante tener en cuenta que en caso de que el supervisor del contrato se desvincule de la Entidad sin que haya cerrado el expediente contractual, deberá entregar una relación de los contratos a su cargo y que se encuentren en esta situación, a su superior jerárquico para su reasignación, seguimiento y control. **s.** Las demás inherentes a la función asignada, contempladas en las Leyes 80 de 1993, 1474 de 2011 y las que sean aplicables, así mismo las señaladas en la Resolución Ministerial No. 6302 de 31 de julio de 2014 *"Por la cual se Adopta expide el Manual de Contratación del Ministerio de Defensa Nacional, y sus Unidades Ejecutoras"*, la cual puede ser consultada en la página web del Ministerio de Defensa Nacional o la Dirección Ejecutiva de la Justicia Penal Militar – MDN. **PARÁGRAFO PRIMERO. - CAMBIO DE SUPERVISOR:** Si se requiere el cambio del supervisor por razones de fuerza mayor o caso fortuito, ausencia temporal o definitiva, o por circunstancias debidamente justificadas, el competente contractual procederá a designar un nuevo supervisor mediante acto administrativo. Si el supervisor en ejercicio se encuentra en condiciones de suscribir un acta lo hará conjuntamente con el designado en su reemplazo, en ésta constará: Estado de ejecución del contrato, relación de documentos que entrega y observaciones que considere pertinentes. Si no es posible la suscripción conjunta del acta, el supervisor entrante dejará constancia del estado en que se encuentre el contrato al asumir el ejercicio de estas funciones. **PARÁGRAFO SEGUNDO – PROCEDIMIENTO EN CASO DE INCONFORMIDAD DEL SUPERVISOR CON RELACIÓN A LA EJECUCIÓN DEL CONTRATO:** De conformidad con lo dispuesto en el Manual de Contratación del Ministerio de Defensa Nacional, cuando el supervisor del contrato se encuentre en desacuerdo con la ejecución y desarrollo de las obligaciones pactadas en el contrato, o con la forma de los actos, documentos o circunstancias examinadas, deberá sin excepción formular todo sus reparos por escrito ante el Grupo de Asesoría Legal de la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN**, con el cumplimiento de los siguientes requisitos: **1)** Los reparos a la ejecución contractual deben ser motivados con razonamientos fundados en hechos, circunstancias y normas en las que se apoye el criterio sustentado y deben comprender todas las observaciones y objeciones correspondientes. **2)** El supervisor deberá reportar los resultados más relevantes de su actuación y recomendará al competente contractual las actuaciones que considere más convenientes u oportunas para la normal ejecución del contrato. **3)** En caso de apreciar graves irregularidades en la ejecución de un contrato que amenace su paralización, es obligación del supervisor informar por escrito dentro delos cinco (5) días hábiles siguientes a la ocurrencia de los hechos al competente contractual y al Coordinador de la dependencia que ha contratado el servicio, con los mismos requisitos en los numerales anteriores. **PARÁGRAFO TERCERO - LIMITACIONES DEL SUPERVISOR:** El supervisor no estará facultado en ningún momento, para adoptar decisiones que impliquen la modificación de los términos y condiciones previstos en el presente contrato, las cuales únicamente podrán ser adoptadas por el competente contractual y el representante legal de **USCOM S.A.S.**, mediante la suscripción de modificaciones al contrato principal. **CLÁUSULA**

DÉCIMA TERCERA - GARANTÍA ÚNICA DE CUMPLIMIENTO: Dentro del término señalado en la plataforma del SECOP II **USCOM S.A.S.**, constituirá la garantía única de cumplimiento y de responsabilidad civil extracontractual que tratan los artículos 2.2.1.2.3.1.7 y 2.2.1.2.3.1.8 del único Reglamentario Decreto 1082 de 2015, a favor de la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MDN** con NIT 900.384.997 –1, que cubra los siguientes amparos:

AMPAROS EXIGIBLES	%	VIGENCIA
Cumplimiento	20%	Con una vigencia igual al plazo de ejecución del contrato y doce (12) meses más, contados a partir de la suscripción de este y de las prórrogas si las hubiere.
Calidad del Servicio	20%	Con una vigencia igual al plazo de ejecución del contrato y doce (12) meses más, contados a partir de la suscripción de este y de las prórrogas si las hubiere.
Calidad y correcto funcionamiento de los bienes	20%	Con una vigencia igual al plazo de ejecución del contrato y doce (12) meses más, contados a partir del acta de recibo a satisfacción del bien y de las prórrogas si las hubiere. Este amparo debe garantizar la calidad y correcto funcionamiento de los bienes que recibe la Entidad Estatal en cumplimiento del contrato.
Pago de salarios, prestaciones sociales legales e indemnizaciones laborales	10%	Con una vigencia igual al plazo de ejecución del contrato y tres (3) años más, contados a partir de la fecha de suscripción de este y de las prórrogas si las hubiere. Este amparo cubre a la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MDN** de los perjuicios que se le ocasionen como consecuencia del incumplimiento de las obligaciones laborales que este obligado **USCOM S.A.S.**, garantizado, derivadas de la contratación del personal utilizado para la ejecución del contrato amparado.
Responsabilidad civil extracontractual	200 SMMLV	En cuantía equivalente a doscientos salarios mínimos mensuales vigentes (200) SMMLV con vigencia igual al plazo de ejecución del contrato y de las prórrogas si a ello hubiere lugar.

PARÁGRAFO PRIMERO: El mecanismo de cobertura del riesgo será la póliza única de cumplimiento y responsabilidad civil extracontractual expedidas por una compañía de seguros legalmente establecida en Colombia que deberá contener los requisitos señalados en la Subsección 1 Sección 3, del artículo 2.2.1.2.3.1.1 y

siguientes del Decreto Único Reglamentario 1082 de 2015. **PARÁGRAFO SEGUNDO:** Si la póliza única de cumplimiento y responsabilidad civil extracontractual son obtenidas a través de un corredor de seguros, se deberá allegar certificación expedida por la compañía aseguradora con el objeto de verificar que la agencia o el agente se encuentre debidamente autorizado por la entidad aseguradora que expide la póliza. **PARÁGRAFO TERCERO:** La póliza única de cumplimiento y responsabilidad civil extracontractual **deberán estar firmadas por la aseguradora y quien firma debe acreditar su calidad mediante certificación expedida por la Superintendencia Financiera de Colombia** (representante legal) o poder otorgado por escritura pública e inscripción en el registro mercantil de la Cámara de Comercio competente (sucursales o apoderados). **PARÁGRAFO CUARTO:** Tratándose de garantías consistentes en pólizas de seguro, éstas no expirarán por falta de pago de la prima o revocatoria unilateral. **PARÁGRAFO QUINTO:** La póliza única de cumplimiento deberá indicar de forma expresa en su texto que se **ampara el cumplimiento del contrato, el pago de las multas, de la cláusula penal pecuniaria convenidas y que la aseguradora renuncia al beneficio de excusión.** **PARÁGRAFO SEXTO: USCOM S.A.S.**, deberá restablecer el valor de la garantía única, cuando ésta se haya visto reducido por razón de las reclamaciones efectuadas por la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN**; de igual manera, en cualquier evento en que se aumente o adicione el valor del contrato y/o se prorrogue su término, deberá ampliar el valor y/o la vigencia de las garantías otorgadas. **PARÁGRAFO SÉPTIMO: USCOM S.A.S.**, se obliga para con la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** a mantener vigente la garantía única hasta la liquidación del contrato en los términos señalados en el artículo 2.2.1.2.3.1.12 del Decreto Único Reglamentario 1082 de 2015 y responsabilidad civil extracontractual hasta el periodo de ejecución del contrato según lo dispuesto en el artículo 2.2.1.2.3.1.17 ibídem. **PARÁGRAFO OCTAVO:** Si **USCOM S.A.S.**, se negare a constituir la garantía, así como a no otorgarla en los términos, cuantía y duración establecidos, la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** podrá aplicar las sanciones contractuales a que haya lugar. **PARÁGRAFO NOVENO: USCOM S.A.S.**, allegará con la póliza única de cumplimiento y responsabilidad civil extracontractual certificado que acredite que se encuentra al día en el pago de aportes parafiscales relativos al Sistema de Seguridad Social Integral, así como los propios del Sena, ICBF y Cajas de Compensación Familiar, cuando corresponda, anexando para ello copia de las dos (2) últimas` Planillas de pago. En caso de que el documento sea suscrito por el revisor fiscal, deberá adjuntar copia de la tarjeta profesional, de la cédula de ciudadanía y del certificado de la Junta Central de Contadores vigente. **PARÁGRAFO DECIMO:** La póliza de responsabilidad extracontractual deberá contener como mínimo en su texto, los amparos señalados en el artículo 2.2.1.2.3.1.8 del Decreto Único Reglamentario 1082 de 2015, esto es: Cobertura básica de predios, labores y operaciones. Cobertura expresa de los perjuicios que cause el asegurado (daño emergente y lucro cesante). Cobertura expresa de perjuicios extra patrimoniales. Cobertura expresa de la responsabilidad surgida por actos de contratistas y subcontratistas (excepto cuando el subcontratista tenga su propio seguro de responsabilidad

extracontractual, con los mismos amparos aquí listados). Cobertura expresa de amparo patronal. Cobertura expresa de vehículos propios y no propios. **CLÁUSULA DÉCIMA CUARTA – SANCIONES EN MATERIA DE ACTUACIONES CONTRACTUALES:** Previa aplicación del precepto constitucional del debido proceso, señalado en el artículo 29 de la Constitución Política, artículo 17 de la Ley 1150 de 2007 y artículo 86 de la Ley 1474 de 2011, la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** con la acreditación de las pruebas correspondientes podrá aplicar las siguientes sanciones: **a) MULTAS**: En caso de incumplimiento total o parcial de alguna de las obligaciones derivadas del presente contrato por causas imputables a **USCOM S.A.S.**, salvo circunstancias de fuerza mayor o caso fortuito conforme a las definiciones del artículo 1° de la Ley 95 de 1890, las partes acuerdan que la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MDN**, mediante acto administrativo, podrá con el objeto de conminar a **USCOM S.A.S.**, a cumplir sus obligaciones, imponer multas cuyo valor se liquidará con base en un cero punto cinco por ciento (0,5%) del valor del contrato, por cada día de retardo y hasta por quince (15) días calendario. Esta sanción se impondrá conforme a la ley y se reportará a la Cámara de Comercio competente. **b) MULTAS POR LA MORA EN LA CONSTITUCIÓN DE LOS REQUISITOS DE PERFECCIONAMIENTO Y EJECUCIÓN:** Cuando **USCOM S.A.S.**, no constituya dentro del término y en la forma prevista en el contrato, o en alguno de sus modificatorios, la garantía única de cumplimiento y de responsabilidad civil extracontractual y/o alguno de los requisitos de ejecución a su cargo, la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** mediante acto administrativo, podrá imponer una multa cuyo valor se liquidará con base en un cero punto dos por ciento (0.2%) del valor del contrato, por cada día de retardo y hasta por diez (10) días calendario, al cabo de los cuales la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** podrá declarar la caducidad. **c) MULTA POR INCUMPLIMIENTO AL SISTEMA DE SEGURIDAD SOCIAL Y PARAFISCALES**: En caso de mora o incumplimiento de las obligaciones frente al Sistema de Seguridad Social Integral y Parafiscales, la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MDN** podrá imponer a **USCOM S.A.S.**, multas cuyo valor se liquidará con base en un cero punto uno por ciento (0,1%) del valor del contrato, por cada día de retardo en la presentación de la certificación que evidencie el cumplimiento de la obligación y hasta por quince (15) días calendario. **d) PENAL PECUNIARIA:** En el evento de declararse la caducidad del contrato o su incumplimiento definitivo, la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN**, mediante acto administrativo motivado, le impondrá a **USCOM S.A.S.**, a título de pena pecuniaria, una suma equivalente al diez por ciento (10%) del valor total del contrato cuando se trate de incumplimiento total del mismo y proporcional al incumplimiento parcial del contrato que no supere el porcentaje señalado. La imposición de esta pena pecuniaria se considerará como pago parcial o definitivo, según corresponda, de los perjuicios que cause a la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN**. No obstante, la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** se reserva el derecho a cobrar los perjuicios causados por encima del monto de lo aquí pactado, siempre que los mismos se acrediten en las condiciones establecidas en el presente contrato, de

conformidad con lo señalado en el artículo 86 de la Ley 1474 de 2011. **PARÁGRAFO PRIMERO.- LEGALIDAD DE LA SANCIÓN:** Estas sanciones se pactan con fundamento en el principio de autonomía de la voluntad previsto en el artículo 40 de la Ley 80 de 1993, y se impondrán respetando el derecho al debido proceso de que trata el artículo 29 de la Constitución Política, el artículo 17 de la Ley 1150 de 2007, y de conformidad con el procedimiento establecido en el artículo 86 de la Ley 1474 de 2011. Una vez en firme la sanción se reportará a la Cámara de Comercio respectiva. **PARÁGRAFO SEGUNDO.-** Se entiende aceptado el contenido de la presente cláusula y su obligatoriedad por parte de **USCOM S.A.S.**, cuando éste último suscribe el contrato. **PARÁGRAFO TERCERO.- PUBLICIDAD DE LA SANCIÓN:** Una vez en firme la sanción, la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MDN** procederá a publicar la parte resolutiva del acto que la declara en el Portal Colombia Compra Eficiente – Sistema Electrónico de Contratación Pública – SECOP II www.colombiacompra.gov.co., y se comunicará a la Cámara de Comercio en que se encuentre inscrito **USCOM S.A.S.** También se comunicará a la Procuraduría General de la Nación. La anterior publicación se hará de conformidad con lo previsto en el artículo 31 de la Ley 80 de 1993, modificado por el artículo 218 del Decreto Ley 019 de 2012. **PARÁGRAFO CUARTO.- APLICACIÓN DEL VALOR DE LAS SANCIONES PECUNIARIAS:** Una vez se termine la audiencia en la que se impone la sanción, a través de resolución motivada que se entenderá notificada y ejecutoriada en dicho acto público, **USCOM S.A.S.**, dispondrá de quince (15) días calendario para proceder de manera voluntaria a su pago. Las multas no serán reintegrables aún en el supuesto que **USCOM S.A.S.**, ejecute la obligación incumplida. En caso de pago voluntario y una vez en firme el respectivo acto administrativo, podrá ejecutarse la garantía contractual o tomarse de saldo a favor de **USCOM S.A.S.**, si los hubiere. Si esto último no fuere posible, se cobrará por vía ejecutiva. **CLÁUSULA DÉCIMA QUINTA - CADUCIDAD ADMINISTRATIVA:** Si se presenta algún hecho constitutivo de incumplimiento de las obligaciones a cargo de **USCOM S.A.S.**, que afecte de manera grave y directa la ejecución del contrato y evidencie que puede conducir a su paralización, la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MDN** por medio de acto administrativo debidamente motivado podrá decretar la caducidad y ordenar la liquidación en el estado en que se encuentre, todo de conformidad con lo previsto en el artículo 18 de la Ley 80 de 1993. Ejecutoriada la resolución de caducidad, el contrato quedará definitivamente terminado y **USCOM S.A.S.**, no tendrá derecho a reclamar indemnización alguna. La **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MDN,** hará efectiva la garantía pactada en el mismo, así como el valor de la pena pecuniaria, y procederá a su liquidación. En el acta de liquidación se determinarán las obligaciones a cargo de las partes, teniendo en cuenta el valor de las sanciones por aplicar o las indemnizaciones a cargo de **USCOM S.A.S.**, si a esto hubiere lugar y la fecha de pago. **CLÁUSULA DÉCIMA SEXTA - OTRAS FACULTADES EXCEPCIONALES:** En caso de presentarse cualquiera de las circunstancias establecidas en los artículos 15, 16 y 17 de la Ley 80 de 1993, y demás normas concordantes, debidamente establecidas y documentadas, la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MDN** podrá hacer uso de las facultades excepcionales allí

previstas. **CLÁUSULA DÉCIMA SÉPTIMA- CESIONES Y SUBCONTRATOS**: **USCOM S.A.S.**, no podrá ceder el presente contrato a persona alguna natural o jurídica, nacional o extranjera, sin previa autorización escrita de la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MDN**, pudiendo éste reservarse las razones para negar dicha autorización. **USCOM S.A.S.**, solo podrá subcontratar parcialmente la ejecución del contrato, en tal caso la celebración de subcontratos no lo relevará de las responsabilidades que asume en virtud del presente contrato. La **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MDN no adquirirá relación alguna con los subcontratistas**. **CLÁUSULA DÉCIMA OCTAVA - CESIÓN DE DERECHOS ECONÓMICOS**: En caso de que **USCOM S.A.S.**, decida efectuar una cesión y/o pignoración de derechos económicos deberá solicitar su aceptación y notificación por parte de la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MDN**, para lo cual deberá anexar como mínimo los siguientes documentos: **1)** Contrato de cesión y/o pignoración de derechos económicos del contrato objeto de la cesión, firmado por el cesionario y el cedente donde se relacione en forma explícita lo siguiente: **a)** Valor de la cesión **b)** Especificar si la cesión obedece al contrato principal y/o contratos adicionales **c)** Aceptación por parte del cesionario de los descuentos de ley cuando aplique. **2)** Acta de junta de socios o documento consorcial, en donde se autorice al representante legal de la figura correspondiente para efectuar la cesión. **3)** Certificado de existencia y representación legal del cesionario y el cedente cuando se trate de persona jurídica y/o certificado de inscripción cuando se trate de persona natural expedido por la Cámara de comercio del domicilio correspondiente. **4)** Certificación bancaria con número de cuenta y beneficiario donde se deben consignar los valores cedidos. **5)** Declaración bajo juramento del cesionario en la cual se exprese el cumplimiento de lo previsto en el Decreto 4334 de 2008, en concordancia con el Decreto 1981 de 1988. **CLÁUSULA DÉCIMA NOVENA – CASO FORTUITO O FUERZA MAYOR:** Las partes quedan exoneradas de responsabilidad por el incumplimiento de cualquiera de sus obligaciones o por la demora en la satisfacción de cualquiera de las prestaciones a su cargo derivadas del presente contrato, cuando el incumplimiento sea resultado o consecuencia de un evento de fuerza mayor o caso fortuito debidamente invocadas y constatadas de acuerdo a la Ley y la jurisprudencia colombiana. **CLÁUSULA VIGÉSIMA – SOLUCIÓN DE CONTROVERSIAS**: Las partes acuerdan que para la solución de las controversias o diferencias que surjan entre **USCOM S.A.S.**, y la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** con ocasión de la firma, ejecución, interpretación, prórroga, terminación o liquidación de este contrato, así como cualquier otro asunto relacionado con el presente contrato, podrán acudir en primer término a los mecanismos directos de solución de controversias contractuales establecidos en la ley. Agotado este requisito sin que logre dirimirse la controversia las partes podrán acudir a la jurisdicción de lo contencioso administrativo. **CLÁUSULA VIGÉSIMA PRIMERA – CAUSALES DE TERMINACIÓN:** Serán causales para dar por terminado el presente contrato las siguientes: **1)** Por mutuo acuerdo entre las partes, solicitud que debe ser presentada mínimo con ocho (8) días de antelación a la fecha de solicitud de terminación anticipada del contrato. **2)** Por el vencimiento del plazo de ejecución. **3)** Por cumplimiento del objeto contractual dentro del plazo de

ejecución establecido o con anterioridad al vencimiento del mismo. **4)** En forma unilateral por parte de la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** conforme a lo establecido en la ley. **5)** Por causas legales. **CLÁUSULA VIGÉSIMA SEGUNDA – SUSPENSIÓN TEMPORAL DEL CONTRATO:** De común acuerdo las partes contratantes podrán suspender la ejecución de este contrato, mediante la suscripción de un acta en la cual conste el evento de suspensión y la fecha de su reinicio sin que para efectos del término de duración del contrato se compute el tiempo de la suspensión. **CLÁUSULA VIGÉSIMA TERCERA - INDEMNIDAD: USCOM S.A.S.**, se obliga para con la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** a mantenerla libre de cualquier daño o perjuicio originado en reclamaciones de terceros y que se deriven de sus actuaciones o de sus subcontratistas o dependientes y realizadas durante la ejecución del contrato. **CLÁUSULA VIGÉSIMA CUARTA - INHABILIDADES E INCOMPATIBILIDADES: USCOM S.A.S.**, con la firma del presente contrato declara bajo la gravedad de juramento que ni él, ni su representante legal, ni sus socios se hallan incursos por sí o por interpuesta persona en las causales de inhabilidad o incompatibilidad señaladas por la Constitución Política, la Ley 80 de 1993, el artículo 18 de la Ley 1150 de 2007, Ley 1474 de 2011 y demás disposiciones que rijan la materia. **PARÁGRAFO ÚNICO: INHABILIDADES E INCOMPATIBILIDADES SOBREVINIENTES:** Si llegare a sobrevenir inhabilidades e incompatibilidades en **USCOM S.A.S.**, éste cederá el contrato previa autorización escrita de la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MDN** o, si ello no fuere posible, renunciará a su ejecución. **CLÁUSULA VIGÉSIMA QUINTA - DOCUMENTOS:** Entre otros, los documentos que a continuación se relacionan se consideran, para todos los efectos, parte integrante del presente contrato y, en consecuencia, producen sus mismos efectos u obligaciones jurídicas y contractuales: **a**) Oficio por el cual se solicita aprobación para adelantar el proceso contractual, autorizado por el Ordenador del Gasto. **b**) Resolución No. 000233 del 30 de octubre de 2020, por medio de la cual se designa a la Gerente e integrantes de unos comités estructurador, evaluador, adquisiciones, así como supervisor, para que actúen conforme a sus funciones en un proceso contractual. **c**) Certificado Plan Anual de Adquisiciones No. 28 MDN-DEJPM-GLAF 40.63 del 23 de julio de 2020, modificado el 16 de octubre del mismo año. **d)** Certificado de Disponibilidad Presupuestal No. 10920 del 23 de julio de 2020, reducido el 15 de octubre y adicionado el 16 octubre del año en curso. **e)** Estudios de mercado junto con las cotizaciones. **f)** Estudios y documentos previos. **g)** Proyecto de pliego de condiciones del Proceso de Selección Abreviada – Subasta Inversa Electrónica No. 043-2020 DEJPM – MDN. **h**) Formularios de preguntas y respuestas Nos. 1 y 2. **i)** Resolución de Apertura No. 000262 del 24 de noviembre de 2020. **j)** Pliego de condiciones definitivo del Proceso de Selección Abreviada – Subasta Inversa Electrónica No. 043-2020 DEJPM- MDN. **k)** Informes de evaluación técnica, jurídica, financiera y organizacional y económica, realizados dentro del Proceso de Selección Abreviada – Subasta Inversa Electrónica No. 043-2020 DEJPM – MDN. **l**) Consolidado de evaluación definitivo de las ofertas del 9 de diciembre de 2020. **m)** Cuadernillos de preguntas y respuestas a las observaciones presentadas al informe de evaluación. **n)** Evento de subasta realizado mediante la plataforma

de Secop II, llevado a cabo los días 10 y 11 de diciembre de 2020. **o)** Resolución de Adjudicación No. 000282 del 14 de diciembre de 2020. **p)** Oferta presentada por **USCOM S.A.S. q**) Acta No. 65 del 14 de diciembre de 2020 del Comité de adquisiciones. **e)** Los demás documentos que se relacionan con el presente contrato de Compraventa. **CLÁUSULA VIGÉSIMA SEXTA. IMPUESTOS: USCOM S.A.S.**, pagará todos los impuestos, tasas, contribuciones y similares derivados de la ejecución del contrato, conforme a la ley colombiana. **CLÁUSULA VIGÉSIMA SÉPTIMA - RÉGIMEN LEGAL:** Este contrato se regirá por el Estatuto General de Contratación de la Administración Pública vigente, Ley 1150 de 2007, Ley 1474 de 2011, el Decreto Único Reglamentario 1082 de 2015, las leyes de presupuesto y, en general, las normas civiles y comerciales vigentes, las demás normas concordantes que rijan o lleguen a regir los aspectos del presente contrato y las disposiciones internas del Ministerio de Defensa Nacional que apliquen. **CLÁUSULA VIGÉSIMA OCTAVA - INFORMACIÓN Y CONFIDENCIALIDAD DE LA INFORMACIÓN:** En virtud del presente contrato **USCOM S.A.S.**, se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del presente contrato, así como sobre los lugares a los cuales tenga acceso con ocasión de su desarrollo. Igualmente, **USCOM S.A.S.**, debe suscribir el Anexo No. 2 "***COMPROMISO DE CONFIDENCIALIDAD DEL CONTRATO***", el cual hace parte integral del contrato. **CLÁUSULA VIGÉSIMA NOVENA - LIQUIDACIÓN:** El presente contrato se liquidará acorde con lo dispuesto en el artículo 60 de la Ley 80 de 1993, modificado por el artículo 217 del Decreto Ley 019 de 2012 y el artículo 11 de la Ley 1150 de 2007. **CLÁUSULA TRIGÉSIMA - MONEDA DEL CONTRATO:** La moneda del presente contrato es la legal colombiana. **CLÁUSULA TRIGÉSIMA PRIMERA – SUJECIÓN A LA LEY COLOMBIANA:** El presente contrato queda sujeto a la ley colombiana. **CLÁUSULA TRIGÉSIMA SEGUNDA - AUTONOMÍA ADMINISTRATIVA Y EXCLUSIÓN DE RELACIÓN LABORAL:** El personal empleado o contratado por **USCOM S.A.S.**, para la ejecución del contrato no tiene ni adquiere ninguna relación de dependencia o subordinación laboral con la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN. CLÁUSULA TRIGÉSIMA TERCERA - PERFECCIONAMIENTO Y EJECUCIÓN:** El presente contrato de Compraventa se entiende perfeccionado a partir de la suscripción del mismo. Para su Ejecución requiere de la expedición del registro presupuestal, aprobación de la garantía única de cumplimiento y de responsabilidad civil extracontractual constituidas por **USCOM S.A.S.**, así como verificación de estar al día en los aportes a la seguridad social y riesgos laborales. El contrato se entiende comunicado a **USCOM S.A.S.**, con la aprobación y firma que se realiza del mismo a través del Sistema Electrónico de Contratación Pública – SECOP II. **CLÁUSULA TRIGÉSIMA CUARTA - AVISOS Y NOTIFICACIONES:** Todas las comunicaciones que se requieran en desarrollo del presente contrato se presentarán por escrito, directamente, por correo certificado, así: las que deba realizar la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** se remitirán al kilómetro 1.5 vía Chía-Cajicá edificio Oxus oficina 301, correo: info@uscom.net.co; las que deba realizar **USCOM S.A.S.**, las remitirá por escrito directamente a la carrera 46 No. 20 C – 1 Cantón Militar Occidental "Coronel Francisco José de Caldas", Puente Aranda, Palacio de la Justicia Penal Militar y Policial "TF. Laura Rocío Prieto Forero" o donde se encuentren ubicadas sus

oficinas. **CLÁUSULA TRIGÉSIMA QUINTA. PUBLICIDAD:** Una vez suscrito el presente contrato, el mismo será publicado en el Portal Único de Contratación SECOP II www.colombiacompra.gov.co. **CLÁUSULA TRIGÉSIMA SEXTA. DOMICILIO CONTRACTUAL:** Para todos los efectos, las partes acuerdan como domicilio contractual la ciudad de Bogotá D.C.; para constancia de lo anterior, se firma en un (1) original a los 16 DIC. 2020

NOTA: El presente contrato será aprobado y firmado por las partes a través de la plataforma del SECOP II; no obstante, se suscribe por parte del Director Ejecutivo de la Justicia Penal Militar y el Representante Legal de USCOM S.A.S.

POR LA DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN,

FABIO ESPITIA GARZÓN
Director Ejecutivo

POR USCOM S.A.S.,

OTTO FRANCISCO URREA JARAMILLO
Representante Legal

Elaboró: PD. Diana Carolina Reyes Pulido

Revisó: Contratista. Ernesto Mario Ibáñez Fernández

PD. Gustavo Avella Ávila – Gerente del Proceso

PD Diego Javier Sánchez Charry– Evaluador Económico

Ing. Luis Alirio Dorado Bravo-Evaluador Técnico

Aprobó: Doctor. José Tobías Betancourt Ladino – Contratista

ANEXO No. 1
ANEXO TÉCNICO DEL CONTRATO

ITEM	NOMBRE	CANTIDAD FINAL	PRESENTACIÓN REQUERIDA
1	**HARDWARE**		
1.1	FIREWALLS NEXT GENERATION CON GARANTÍA MINIMA UN AÑO, INCLUIDO LOS ACCESORIOS NECESARIOS PARA EL HA.	2	Unidad
1.2	(2) DOS UNIDADES DE MÓDULOS SFP+ 1GB Y DOS UNIDADES SFP+ 10GB, POR CADA EQUIPO QUE HAGA PARTE DEL CLUSTER, INCLUIDO CABLES DE CONEXIÒN.	8	Unidad
NOMBRE COMERCIAL	**FIREWALLS NEXT GENERATION**		
MARCA	FORTINET		
MODELO	Firewall FortiGate FG-1101E BDL-950-12, Consola FortiAnalyzer FAZ-200F con FC-10-L200F-247-02-12 y FC-10-L200F-149-02-12		
2.	**LICENCIAMIENTO POR UN (1 AÑO) DEL FIREWALL.**		
2.1	LICENCIAMIENTO CONTROL DE APLICACIONES.	2	Unidad
2.2	LICENCIAMIENTO PREVENCION DE AMENAZAS – IPS PROXIMA GENERACION, ANTIVIRUS DE RED, ANTISPYWARE-	2	Unidad
2.3	LICENCIAMIENTO FILTRADO WEB.	2	Unidad
2.4	LICENCIAMIENTO PREVENCION AMENAZAS DIA CERO	2	Unidad
3.	**SERVICIOS DE MANTENIMIENTO, GESTIÓN, SOPORTE, BOLSA DE HORAS.**		
3.1	MIGRACIÓN DE LA PLATAFORMA ACTUAL, MARCA CHECKPOINT COMPRENDIDA POR LOS SIGUIENTES ELEMENTOS: • DOS (02) FIREWALL NGFW 4800 VERSIÓN R77.30 • UN (01) MANAGEMENT VIRTUAL OPEN SERVER VERSIÓN R80.20 • UN (01) EVENTIA REPORT VIRTUAL OPEN SERVER VERSIÓN R80.20 A LA NUEVA SOLUCIÓN OFERTADA.	1	Unidad
3.2	SOPORTE A INCIDENTES DE 1 Y 2 NIVEL EN MODALIDAD 7X24 PARA LOS DOS (2) FIREWALL POR UN AÑO DIRECTAMENTE DEL FABRICANTE.	1	Unidad
3.3	BOLSA DE 192 HORAS DE ASISTENCIA EN SITIO Y/O REMOTO PARA LA ADMINISTRACIÓN DE LA SOLUCIÓN.	192	HORAS

<table>
<tr><th colspan="2">CONDICIONES TÉCNICAS MÍNIMAS REQUERIDAS</th></tr>
<tr><th>1.</th><th>DESCRIPCIÓN GENERAL</th></tr>
<tr><td>1.1.</td><td>
a. Adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la información perimetral que incluye filtro de paquetes, control de aplicaciones, administración de ancho de banda (QoS), VPN IPSec y SSL, IPS, prevención contra amenazas de virus, spyware y malware "Zero Day", controles de transmisión de datos y acceso a internet componiendo una plataforma de seguridad integrada y robusta.
b. USCOM S.A.S., deberá realizar la migración de la plataforma actual, marca checkpoint comprendida por los siguientes elementos:
▪ Dos (02) firewall NGFW 4800 versión R77.30.
▪ Un 01 (01) Management virtual open server versión R80.20.
▪ Un (01) eventia report virtual open server versión R80.20.
Dentro de las actividades de migración e implementación se deberán configurar las reglas existentes de filtrado para las redes utilizadas por la Entidad.
c. En los Firewall actuales se encuentran interconectan con los switches de marca Dell Force10 S-25N y la nueva solución de seguridad deberá permitir realizar la conexión con estos mismos switches.
a. En la actualidad se tienen las siguientes configuraciones en los Firewall de la Entidad que se debe migrar a la nueva solución de protección.
▪ Objetos de red 7000.
▪ Aplicaciones y categorías 10.000.
▪ servicios 1000 y 100 usuarios.
▪ VPN site to site 5.
▪ Reglas de seguridad 150.
▪ Reglas de aplicación 60.
▪ Reglas de NAT 120.

b. Las características generales de Hardware, Software y servicios mínimos requeridos son:
<table>
<tr><th>DESCRIPCIÓN</th><th>TIPO</th><th>CANT</th></tr>
<tr><td>Firewall NGFW con fuentes de alimentación de CA redundantes, consolas de administración monitoreo y reportes.</td><td>HARDWARE</td><td>2</td></tr>
<tr><td>Soporte de fábrica (1) un año</td><td>SOPORTE</td><td>2</td></tr>
<tr><td>Incluir conector transceivers SFP 1 Gb alcance mínimo de 550m tipo SX</td><td>HARDWARE</td><td>4</td></tr>
<tr><td>Incluir conector transceivers SFP+ 10 Gb alcance mínimo de 300m tipo SR</td><td>HARDWARE</td><td>4</td></tr>
<tr><td>Incluir conector para establecer la conexión HA entre los 2 equipos NGFW a mínimo 10Gb</td><td>HARDWARE</td><td>1</td></tr>
<tr><td>Suscripción de prevención de amenazas para el dispositivo en un par HA año 1</td><td>SOFTWARE</td><td>2</td></tr>
<tr><td>Suscripción de filtrado de URL para dispositivo en un par HA año 1</td><td>SOFTWARE</td><td>2</td></tr>
<tr><td>Suscripción cloud de análisis, detección y bloqueo de ataques complejos de amenazas desconocidas, malware y los exploits de día cero, consola de administración, monitoreo y reportes.</td><td>SOFTWARE</td><td>2</td></tr>
</table>
</td></tr>
</table>

	Implementación de dos (2) Firewall en HA	SERVICIOS	1
	Socialización de la operación del Firewall para máximo 4 personas del área de TI. Tiempo de duración: 40 horas	SERVICIOS	1
	Soporte a incidentes de 1 y 2 nivel en modalidad 7X24 de dos (2) Firewall en HA, de la consola de administración, monitoreo y reportes.	SERVICIOS	1
	Bolsa de 192 horas de asistencia en sitio y/o remoto para la administración de la solución, ataques, fallos o problemas que afecten la solución, que no incluye el fabricante.	SERVICIOS	1
1.2.	La solución de Firewall debe contar con una herramienta que convierta desde múltiples fabricantes de firewall, como mínimo desde Checkpoint con destino al formato de la solución adquirida y además optimice las políticas para poder convertir las reglas de origen, destino y puerto en reglas de NGFW basadas en aplicación aprendiendo del tráfico de la red o basado en técnicas de inteligencia artificial.		
1.3.	Por el equipamiento que compone la plataforma de seguridad, se entiende el hardware y el licenciamiento de software necesarios para su funcionamiento.		
1.4.	Por consola de administración y monitoreo, se entiende el licenciamiento de software necesario para las dos funcionalidades, también como el hardware dedicado para el funcionamiento de las mismas.		
1.5.	La consola de administración y monitoreo de la solución de seguridad deben contar con los recursos de CPU, memoria, interfaz de red y sistema operacional dedicados para esta función, independientes de los recursos del Firewall, las cuales pueden ser fiscos virtuales o dentro del mismo chasis.		
1.6.	La solución de Firewall y las consolas debe soportar mínimo el 30% de crecimiento de tráfico proyectado por la Entidad en los equipos ofertados, sin que se requiera la adquisición de recursos adicionales, es decir, sin costo para la Dirección Ejecutiva de la Justicia Penal Militar –MDN.		
1.7.	El sistema de seguridad deberá permitir la configuración de 10.000 objetos		
1.8.	Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar en listados en el sitio del fabricante como listas de fin de vida (end-of-life), fin de venta (end-of-sale) o fin de soporte (end-support).		
1.9.	El fabricante debe estar en el cuadrante de líderes de Gartner para "Enterprise Firewall" o firewalls empresariales en alguno de los últimos 5 años.		
1.10.	El fabricante debe estar como mínimo en el cuadrante Strong Performers del informe de Forrester de "Zero Trust eXtended (ZTX) Ecosystem Providers o que esté recomendado en estudios de NSS Labs para NGFW.		
1.11.	La plataforma de Firewall debe estar certificado para IPv6 en Firewall e IPS por USGv6 y soportar dual stack ipv4/ipv6.		
1.12.	La solución debe consistir en appliances de seguridad de red con funcionalidades de Next Generation Firewall (NGFW), y consola de administración y monitoreo;		
1.13.	Por funcionalidades de NGFW se entiende: reconocimiento de aplicaciones, prevención de amenazas, prevención de intrusos, identificación de usuarios y control granular de permisos.		
1.14.	La plataforma debe ser optimizada para análisis de contenido de aplicaciones en Capa 7.		
1.15.	Debe procesar e inspeccionar aplicaciones que utilicen HTTP/2.		

1.16.	El hardware y software que ejecuten las funcionalidades de seguridad de red y de administración y monitoreo, deben ser provistos con recursos propios de **USCOM S.A.S.**, virtualizado o en la nube a través de protocolos seguros. No serán aceptados equipamientos servidores y sistema operacional de uso genérico
1.17.	Todos los equipamientos ofrecidos deben ser adecuados para montaje en rack 19".
1.18.	Los dispositivos de seguridad de red deben poseer por lo menos las siguientes funcionalidades: ▪ Soporte a 4094 VLAN Tags 802.1q; tanto por dispositivo como en una sola interfaz; ▪ Agregación de links 802.3ad. ▪ Policy based routing o policy based forwarding. ▪ Ruteo multicast (PIM-SM). ▪ DHCP Relay. ▪ DHCP Server. ▪ Jumbo Frames. ▪ Soporte a creación de objetos de red que puedan ser utilizados como dirección IP de interfaces L3.
1.19.	Soportar sub-interfaces ethernet lógicas.
1.20.	Debe soportar los siguientes tipos de NAT: ▪ Nat dinámico (Many-to-1). ▪ Nat dinámico (Many-to-Many). ▪ Nat estático (1-to-1). ▪ NAT estático (Many-to-Many). ▪ Nat estático bidireccional 1-to-1. ▪ Traducción de porta (PAT). ▪ NAT de Origen. ▪ NAT de Destino. ▪ Soportar NAT de Origen y NAT de Destino[1] simultáneamente.
1.21.	Enviar log para sistemas de monitoreo externos, simultáneamente.
1.22.	Debe tener la opción de enviar logs para los sistemas de monitoreo externos vía protocolo TCP y SSL.
1.23.	Debe permitir configurar certificado caso necesario para autenticación del sistema de monitoreo externo de logs.
1.24.	Seguridad contra anti-spoofing adress spoofing.
1.25.	Para IPv4, debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).
1.26.	Debe soportar MP-BGP.
1.27.	Para IPv6, debe soportar enrutamiento estático y dinámico (OSPFv3). Soportar OSPF graceful restart.
1.28.	Debe ser capaz de balancear varios enlaces de internet sin el uso de politicas especificas, permitiendo aplicar una variedad de algoritmos distintos (round Robin, weighted).
1.29.	Soportar BFD (bidirectional forward detection).
1.30.	Soportar LACP/LLDP Pre-negotiation.
1.31.	Soportar como minimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Desencripción SSL y SSH, PBR (Policy Base Routing) o PBF (Policy Based

[1] Ver definición en https://blog.ragasys.es/nat-network-address-translation#:~:text=NAT%20en%20Origen%20o%20Source,una%20IP%20de%20origen%20diferente.&text=NAT%20en%20Destino%20o%20Destination,una%20IP%20de%20destino%20diferente.

	Forwarding), QoS, DHCPv6 Relay, Activo/Activo, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones.
1.32.	Los dispositivos de seguridad deben tener la capacidad de operar de forma simultánea mediante el uso de sus interfaces físicas en los siguientes modos dentro del mismo firewall, sin necesidad de tener que hacer uso de contextos virtuales: Modo sniffer (monitoreo y análisis del tráfico de red), Capa 2 (L2), Capa 3 (L3) y modo Transparente; Modo Sniffer, para inspección vía puerto espejo del tráfico de datos de la red.
1.33.	Modo Capa – 2 (L2), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación.
1.34.	Modo Capa – 3 (L3), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación operando como default Gateway de las redes protegidas.
1.35.	Modo Transparente, para poder inspeccionar datos en línea y tener visibilidad del control de tráfico en topologías que no requieran switching y/o routing.
1.36.	Modo mixto de trabajo Sniffer, Transparente, L2 e L3 simultaneamente en diferentes interfaces físicas del mismo equipo. ▪ En el modo Transparente, debe poder soportar al menos 256 interfaces (físicas y/o virtuales) sobre cada sistema virtual lógico (Contexto).
1.37.	Debe contar con una herramienta para optimizar políticas de seguridad, detectar cuáles no se estén usando y por cuánto tiempo; poder aprender de las políticas aplicadas y sugerir que aplicaciones deberían aplicarse a las políticas en el NGFW. Dar estadísticas de uso, ancho de banda por aplicación, último hit de las aplicaciones, sobre cada política, con el objetivo de optimizar y mejorar la configuración del NGFW.
1.38.	Soporte a configuración de alta disponibilidad Pasivo e Activo/Activo: En modo transparente. En layer 3.
1.39.	La configuración en alta disponibilidad debe sincronizar: Sesiones. ▪ Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QOS y objetos de red. ▪ Certificados de desencripción. ▪ Asociaciones de Seguridad de las VPNs. ▪ Tablas FIB. ▪ El HA (modo de Alta-Disponibilidad) debe posibilitar monitoreo de fallo de link.
1.40.	Las funcionalidades de control de aplicaciones, VPN IPSec y SSL, QOS, SSL y SSH Decryption y protocolos de enrutamiento dinámico deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.
1.41.	Debe poder inspeccionar protocolos como: ▪ GRE ▪ IPSEC no encriptado (NULL o AH) ▪ GPRS para GTP-U
1.42.	**a.** **USCOM S.A.S.**, debe realizar la sensibilización en la operación del Firewall para cuatro (4) personas del Área TICs de la Dirección Ejecutiva de la Justicia Penal Militar –MDN. **b.** El temario de la sensibilización será desarrollado mínimo en 40 horas. **c.** La sensibilización se realizara presencial en las instalaciones de **USCOM S.A.S.**, o centro autorizado del fabricante, o virtual programa que debe estar avalado por el fabricante.

	d. El contenido de la sensibilización deberá contener como minimo lo siguiente: • Introducción a NGF • Identificando la topologia del laboratorio • NGF como empresa y sus servicios de seguridad • Configurando el NGF por primera vez para gestión • Configurando el NGF por primera vez para gestión • Revisar y realizar Upgrade del Firewall NGF • Licenciamiento del Firewall NGF • Como crear una regla de seguridad y su funcionalidad • Como crear un NAT • Asignación de direccionamiento IP a las interfaces • Configurando una interface fisica para garantizar la salida a internet • Crear reglas de seguridad para permisos especiales sobre aplicaciones. • Reconociendo el filtrado de contenido
2.	**DESCRIPCIÓN DEL HARDWARE A ADQUIRIR**
2.1.	Por plataforma de seguridad se entiende hardware y software integrados de tipo appliance de propósito especifico.
2.2.	La solución se debe configurar en alta disponibilidad, la alta disponibilidad se entiende como una solución redundante de por lo menos 2 (dos) appliances que cada uno cumpla con las caracteristicas minimas mencionadas en estas especificaciones. Si el oferente para poder cumplir con los requerimientos ofrece N appliance, para poder lograr la alta disponibilidad deberá ofertar N * 2 (dos) appliances.
2.3.	En relación al RMA el fabricante debe disponer de las partes o equipos completos con presencia local en el pais y poder ofrecer minimo reemplazo de partes en el próximo dia hábil, conocido por las siglas en ingles NBD (next business day), para poder garantizar el funcionamiento de la solución.
2.4.	La solución deberá garantizar respaldo y escalabilidad técnica por lo tanto deberá pertenecer al segmento Enterprise Firewall.
2.5.	Las especificaciones técnicas de la solución deberán ser confirmadas mediante documentación oficial de acceso público (guias de administración, manuales y/o guías técnicas). No se aceptarán documentos generados expresamente para este proceso.
2.6.	Las soluciones requeridas deben poder interoperar sin necesidad de software o interacción de terceros.
2.7.	Las soluciones ofrecidas tienen que ser de un mismo fabricante y tener la posibilidad de integrarlas entre si y compartir una misma base de inteligencia, no se aceptan soluciones que no se integren o con bases de firmas de terceras partes.
3.	**CAPACIDAD DE LOS APPLIANCES**
3.1.	Cada appliance de la plataforma de seguridad debe poseer las capacidades y caracteristicas minimas descritas a continuación: ▪ Throughput de **7 Gbps** real de capa 7 con la funcionalidad de control de aplicaciones habilitada, para todas las firmas que el fabricante posea actualizadas con la última actualización disponible. ▪ Throughput de **5 Gbps** real de capa 7 con tráfico real, con las siguientes funcionalidades habilitadas simultáneamente: clasificación y control de aplicaciones, IPS, Control de navegación por URL, control de archivos Antivirus y Antispyware, Control de amenazas avanzadas de día cero (Sandboxing). Para todas las firmas que la plataforma de seguridad posea totalmente activadas, actualizadas al día y con el mayor nivel de seguridad posible; considerando

	múltiples políticas de seguridad (por lo menos 90% de las políticas de seguridad aplicadas), y que tengan habilitado la generación de Logs y NAT aplicado a todas las reglas.
3.2.	Soporte como mínimo, 1 millón de conexiones simultaneas con todos los módulos de seguridad de capa 7 habilitados simultáneamente, en el mayor nivel de seguridad.
3.3.	Soporte mínimo de rendimiento de VPN Ipsec deberá ser mínimo a 5 Gbps.
3.4.	Soporte a, como mínimo, 57.000 nuevas conexiones por segundo;
3.5.	Capacidad de desencripción de SSL de al menos 100.000 sesiones simultaneas.
3.6.	Fuente de energía redundante y hotswap 120 AC;
3.7.	Se requiere que cada equipo tenga conexión a 120 volt o a 240 volt de corriente alterna, con sus respectivos aditamentos de cableado para su conexión.
3.8.	Flujo de ventilación de datacenter del estilo "Front-to-back"
3.9.	Ventiladores redundantes.
3.10.	Se requiere que cada equipo disponga de una disipación de calor mínima de 900 unidades medido en BTU por hora, con una variación de +/- 5%.
3.11.	Disco Solid State Drive (SSD) como mínimo 1x240 GB para el sistema y uso de la solución, con algún nivel de RAID o configuración de respaldo
3.12.	La solución de seguridad debe contar con memoria mínimo DDR4 ECC para soportar la solución y las funcionalidades requeridas, sin costo adicional para la entidad.
4.	**INTERFACES Y CONECTIVIDAD DE LOS APPLIANCES**
4.1.	A continuación, se detallan las Interfaces de red requeridas libres para su uso, es decir, disponer de las mismas luego del armado de la alta disponibilidad y suministrar el cableado necesario de red y eléctrico en caso de ser necesario.
4.2.	Mínimo 8 (ocho) interfaces de red 100/1.000 sobre interfaces de cobre existentes en la actualidad; por equipo. Exceptuando las interfaces de consola, alta disponibilidad y administración, el oferente deberá incluir los patch cord correspondientes categoria 6A certificados de 6mts cada uno con su correspondiente marquilla. El oferente deberá contemplar la interconexión con los switches Dell Force10 S-25N que actualmente tiene la Dirección Ejecutiva en la Justicia Penal Militar – MDN.
4.3.	Mínimo 4 (cuatro) interfaces de red 1 Gbps SFP; por equipo. Exceptuando las interfaces de consola, alta disponibilidad y administración.
4.4.	El oferente deberá entregar con la solución mínimo 2 (dos) SFP ópticos 1Gb por cada equipo con su respectivo patch cord de fibra de 6 metros
4.5.	Mínimo 4 (cuatro) interfaces de red 10G SFP+. Por equipo. Exceptuando las interfaces de consola, alta disponibilidad y administración.
4.6.	El oferente deberá entregar con la solución mínimo 2 (dos) SFP+ ópticos 10Gb por cada equipo con su respectivo patch cord de fibra de 6 metros
4.7.	Cada appliances deberá contar con mínimo 1 (una) interfaces de 1 Gbps SFP+; esta interface deberá ser dedicada para el armado del HA.
4.8.	Cada appliance deberá contar con mínimo una interface de 1 Gbps (cobre) dedicada al respaldo del esquema de alta disponibilidad configurado en el numeral 4.7.
4.9.	1 (una) interface de red 1 Gbps dedicada para administración.
4.10.	1 (una) interface de tipo consola o similar;
4.11.	Soporte a, como mínimo, 10 (diez) ruteadores virtuales.
4.12.	Soporte a, como mínimo, 200 (doscientas) zonas de seguridad.

<table>
<tr><td>4.13.</td><td>Estar en capacidad para soportar sin uso de licenciamiento, 1.000 (mil) clientes de VPN SSL e IPSec simultáneos del estilo cliente-servidor.</td></tr>
<tr><td>4.14.</td><td>Estar en capacidad para soportar sin uso de licenciamiento, 4.000 (cuatro mil) túneles de VPN IPSEC simultáneos del estilo sitio-a-sitio.</td></tr>
<tr><td>5.</td><td>DESCRIPCIÓN DEL LICENCIAMIENTO A ADQUIRIR</td></tr>
<tr><td>5.1.</td><td>A continuación, se detalla el licenciamiento a adquirir:
<table>
<tr><th>DESCRIPCIÓN</th><th>TIPO</th><th>CANT</th></tr>
<tr><td>Suscripción de prevención de amenazas para el dispositivo en un par HA año 1</td><td>SOFTWARE</td><td>2</td></tr>
<tr><td>Suscripción de filtrado de URL para dispositivo en un par HA año 1</td><td>SOFTWARE</td><td>2</td></tr>
<tr><td>Suscripción cloud de análisis, detección y bloqueo de ataques complejos de amenazas desconocidas, malware y los exploits de dia cero, consola de administración, monitoreo y reportes.</td><td>SOFTWARE</td><td>2</td></tr>
</table></td></tr>
<tr><td>5.2.</td><td>El soporte y licencias ofrecido por el fabricante de la solución deben tener vigencia de 1 (un) año en la modalidad 7x24.</td></tr>
<tr><td>5.3.</td><td>El software de la solución deberá ser ofrecido en su versión más estable y/o más avanzada.</td></tr>
<tr><td>6.</td><td>CONTROL DE POLITICAS</td></tr>
<tr><td>6.1.</td><td>Deberá soportar controles por zona de seguridad.</td></tr>
<tr><td>6.2.</td><td>Controles de políticas por puerto y protocolo.</td></tr>
<tr><td>6.3.</td><td>Control de políticas por aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones.</td></tr>
<tr><td>6.4.</td><td>Control de políticas por usuarios, grupos de usuarios, IPs, redes y zonas de seguridad.</td></tr>
<tr><td>6.5.</td><td>Control de políticas por código de País (Por ejemplo: AR, BR, USA, UK, RUS).</td></tr>
<tr><td>6.6.</td><td>Control, inspección y desencripción de SSL por política para tráfico de entrada (Inbound) y Salida (Outbound).</td></tr>
<tr><td>6.7.</td><td>Debe soportar offload de certificado en inspección de conexiones SSL de entrada (Inbound).</td></tr>
<tr><td>6.8.</td><td>Capacidad de Desencripción de SSL de al menos 100.000 sesiones simultaneas.</td></tr>
<tr><td>6.9.</td><td>Debe desencriptar tráfico Inbound y Outbound en conexiones negociadas con TLS 1.2.</td></tr>
<tr><td>6.10.</td><td>Debe desencriptar tráfico que use certificados ECC (como ECDSA)</td></tr>
<tr><td>6.11.</td><td>Control de inspección y desencripción de SSH por política.</td></tr>
<tr><td>6.12.</td><td>La plataforma de seguridad debe implementar copia del tráfico desencriptado (SSL y TLS) para soluciones externas de análisis (Forense de red, DLP, Análisis de Amenazas, entre otras).

Se permite el uso de appliance externo, específico para la desencripción de (SSL y TLS), con copia del tráfico desencriptado tanto para el firewall, como para otras soluciones de análisis externas.</td></tr>
<tr><td>6.13.</td><td>Bloqueos de los siguientes tipos de archivos: bat, cab, dll, exe, pif, y reg, msi, vb, vbe, vbs, jar, cmd, ws, wcs, wsf, js, jse, hta, crt, inf, xsl, cpl, com, wav, htm, html, txt, 7z, gzip, gz, tar.gz, tgz, bz, bz2, tar.bz2, tbz, tbz2, tb2, lzo, lbr, jpeg, jpg, cab, ico, mpeg, asf, swf, chm, dmf, lnk, rar, ps, tar, zip, xml,</td></tr>
<tr><td>6.14.</td><td>Traffic shaping QoS basado en políticas (Prioridad, Garantía y Máximo).</td></tr>
</table>

6.15.	QoS basado en políticas para marcación de paquetes (diffserv marking), inclusive por aplicaciones.
6.16.	Soporte a objetos y Reglas IPV6.
6.17.	Soporte a objetos y Reglas multicast.
6.18.	Soportar los atributos de agendamiento de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.
7.	**CONTROL DE APLICACIONES**
7.1.	Los dispositivos de seguridad de red deberán poseer la capacidad de reconocer aplicaciones, independiente del puerto y protocolo, con las siguientes funcionalidades:
7.2.	Debe ser posible la liberación y bloqueo solamente de aplicaciones sin la necesidad de liberación de puertos y protocolos.
7.3.	Reconocer por lo menos 3000 aplicaciones diferentes, incluyendo, más no limitado: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, video, proxy, mensajería instantánea, compartición de archivos, e-mail.
7.4.	Reconocer por lo menos las siguientes aplicaciones: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, onedrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc.
7.5.	Debe inspeccionar el payload del paquete de datos con el objetivo de detectar a través de expresiones regulares firmas de aplicaciones conocidas por los fabricantes independiente del puerto y protocolo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, incluyendo, más no limitando a RDP en el puerto 80 en vez del 389.
7.6.	Debe detectar aplicaciones a través de análisis del comportamiento del tráfico observado, incluyendo aplicaciones que utilizan cifrado propietario.
7.7.	Identificar el uso de tácticas evasivas, o sea, debe tener la capacidad de visualizar y controlar las aplicaciones y los ataques que utilizan tácticas evasivas vía comunicaciones cifradas, tales como Skype y ataques mediante el puerto 443.
7.8.	Para tráfico Cifrado (SSL y SSH), debe permitir la desencripción de paquetes con el fin de posibilitar la lectura del payload para chequeo de firmas de aplicaciones conocidas por el fabricante.
7.9.	Debe realizar decodificación de protocolos con el objetivo de detectar aplicaciones encapsuladas dentro del protocolo y validar si el tráfico corresponde con la especificación del protocolo, incluyendo, más no limitado a Yahoo! Instant Messenger usando HTTP. La decodificación de protocolo también debe identificar funcionalidades específicas dentro de una aplicación, incluyendo, más no limitado a la compartición de archivos dentro de Webex. También debe detectar el archivo y otros contenidos que deben ser inspeccionados de acuerdo a las reglas de seguridad implementadas.
7.10.	Debe identificar el uso de tácticas evasivas vía comunicaciones cifradas.
7.11.	Debe actualizar la base de firmas de aplicaciones automáticamente. Debe reconocer aplicaciones en IPv6.
7.12.	Limitar el ancho de banda (download/upload) usado por aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos del LDAP/AD.
7.13.	Los dispositivos de seguridad de red deben poseer la capacidad de identificar al usuario de red con integración al Microsoft Active Directory, sin la necesidad de instalación de agente en el Domain Controller, ni en las estaciones de los usuarios.

7.14.	Debe ser posible adicionar control de aplicaciones en todas las reglas de seguridad del dispositivo, o sea, no limitándose solamente a la posibilidad de habilitar control de aplicaciones en algunas reglas.
7.15.	Debe soportar múltiples métodos de identificación y clasificación de las aplicaciones, por lo menos chequeo de firmas, decodificación de protocolos y análisis heurístico.
7.16.	Para mantener la seguridad de la red eficiente, debe soportar el control sobre aplicaciones desconocidas y no solamente sobre aplicaciones conocidas.
7.17.	Permitir nativamente la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias en la propia interface gráfica de la solución, sin la necesidad de acción por parte del fabricante, manteniendo la confidencialidad de las aplicaciones de la empresa.
7.18.	La creación de firmas personalizadas debe permitir el uso de expresiones regulares, contexto (sesiones o transacciones), usando la posición en el payload de los paquetes TCP y UDP y usando decoders de por lo menos los siguientes protocolos:
7.19.	HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP y File body.
7.20.	El fabricante debe permitir la solicitud de inclusión de aplicaciones en la base de firmas de aplicaciones.
7.21.	Debe alertar al usuario cuando una aplicación fuera bloqueada.
7.22.	Debe posibilitar que el control de puertos sea aplicado para todas las aplicaciones.
7.23.	Debe posibilitar la diferenciación de tráficos Peer2Peer (Bittorrent, emule, neonet, etc.) proveyendo granularidad de control/politicas para los mismos.
7.24.	Debe posibilitar la diferenciación de tráficos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) proveyendo granularidad de control/políticas para los mismos.
7.25.	Debe posibilitar la diferenciación y control de partes de las aplicaciones como por ejemplo permitir Gtalk chat y bloquear la transferencia de IM (mensajeria instantánea).
7.26.	Debe posibilitar a diferenciación de aplicaciones Proxies (ghostsurf, freegate, etc.) proveyendo granularidad de control/politicas para los mismos.
7.27.	Debe crear grupos estáticos de aplicaciones cómo Aplicaciones de correo electrónico, para el intercambio de archivos, CRMs, Redes sociales (Facebook, Linkedin), aplicaciones de acceso remoto (Team Viewer, etc).y grupos dinámicos de aplicaciones basados en caracteristicas de las aplicaciones como videoconferencia y mensajería (Teams, Whats app, entre otras).
7.28.	Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc).
7.29.	Nivel de riesgo de las aplicaciones.
7.30.	Categoría y sub-categoria de aplicaciones.
7.31.	Aplicaciones que usen técnicas evasivas, utilizadas por malware, como transferencia de archivos y/o uso excesivo de ancho de banda, etc.
7.32.	Debe poder monitorear aplicaciones SaaS (Software as a service) tanto via GUI como en reporte predefinido.
8.	**PREVENCIÓN DE AMENAZAS**
8.1.	Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS, Antivirus y Anti-Spyware integrados en el propio appliance de Firewall.
8.2.	Debe incluir firmas de prevención de intrusos (IPS) y bloqueo de archivos maliciosos (Antivirus y Anti-Spyware).

8.3.	Las funcionalidades de IPS, Antivirus y Anti-Spyware deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.
8.4.	Debe sincronizar las firmas de IPS, Antivirus, Anti-Spyware cuando esté implementado en alta disponibilidad Activo/Activo.
8.5.	Cuando se utilicen las funciones de IPS, Antivirus y Anti-spyware, el equipamiento debe entregar el mismo performance (no degradar) entre tener 1 única firma de IPS habilitada o tener todas las firmas de IPS, Anti-Vírus y Antispyware habilitadas simultáneamente.
8.6.	Las firmas deben poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo.
8.7.	Excepciones por IP de origen o de destino deben ser posibles en las Reglas, de forma general y firma por firma.
8.8.	Debe soportar granularidad en las políticas de IPS Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos esos ítems.
8.9.	Debe permitir el bloqueo de vulnerabilidades.
8.10.	Debe permitir el bloqueo de exploits conocidos.
8.11.	Debe incluir seguridad contra ataques de negación de servicios.
8.12.	Deberá poseer los siguientes mecanismos de inspección de IPS:
8.13.	Análisis de parones de estado de conexiones.
8.14.	Análisis de decodificación de protocolo.
8.15.	Análisis para detección de anomalías de protocolo.
8.16.	Análisis heurístico.
8.17.	Re-ensamblado de paquetes de TCP.
8.18.	Bloqueo de paquetes malformados.
8.19.	Ser inmune y capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc.
8.20.	Detectar y bloquear el origen de portscans.
8.21.	Bloquear ataques efectuados por worms conocidos, permitiendo al administrador adicionar nuevos patrones.
8.22.	Soportar los siguientes mecanismos de inspección contra amenazas de red: análisis de patrones de estado de conexiones, análisis de decodificación de protocolo, análisis para detección de anomalías de protocolo, análisis heurístico, IP Defragmentation, re-ensamblado de paquetes de TCP y bloqueo de paquetes malformados.
8.23.	Posea firmas específicas para la mitigación de ataques DoS.
8.24.	Posea firmas para bloqueo de ataques de buffer overflow.
8.25.	Posea firmas de C2 (comando y control) generadas de forma automática.
8.26.	Deberá posibilitar la creación de firmas configurables por la interfaz gráfica y/o línea de comando del producto.
8.27.	Permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, HTTP/2, FTP, SMB, SMTP e POP3.
8.28.	Soportar bloqueo de archivos por tipo.
8.29.	Identificar y bloquear comunicaciones como botnets.
8.30.	Debe soportar varias técnicas de prevención, incluyendo Drop y tcp-rst (Cliente, Servidor y ambos).
8.31.	Debe soportar referencia cruzada como CVE.
8.32.	Registrar en la consola de monitoreo las siguientes informaciones sobre amenazas identificadas.

8.33.	Debe soportar la captura de paquetes (PCAP), por firma de IPS y Antispyware.
8.34.	Debe permitir que en la captura de paquetes por firmas de IPS y Antispyware sea definido el número de paquetes a ser capturados. Esta captura debe permitir seleccionar, como mínimo, 50 paquetes.
8.35.	Debe poseer la función resolución de direcciones vía DNS, para que conexiones como destino a dominios maliciosos sean resueltas por el Firewall como direcciones (IPv4 e IPv6), previamente definidos.
8.36.	Permitir el bloqueo de virus, por al menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3.
8.37.	Los eventos deben identificar el país de donde partió la amenaza.
8.38.	Debe incluir seguridad contra virus en contenido HTML y JavaScript, software espía (spyware) y worms.
8.39.	Seguridad contra downloads involuntarios usando HTTP de archivos ejecutables maliciosos.
8.40.	Rastreo de virus en pdf.
8.41.	Debe permitir la inspección en archivos comprimidos que utilizan o algoritmo deflate (zip, gzip, etc.).
8.42.	Debe ser posible la configuración de diferentes politicas de control de amenazas y ataques basados en políticas del firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc, o sea, cada política de firewall podrá tener una configuración diferente de IPS, siendo esas políticas por usuarios, grupos de usuario, origen, destino, zonas de seguridad.
8.43.	De contar con mecanismo Sinkhole DNS para ayudar a identificar hosts infectados en la red protegida mediante el tráfico de DNS en situaciones en las que el firewall no puede ver la consulta DNS del cliente infectado (es decir, el firewall no puede ver el autor de la consulta DNS). El mecanismo sinkkole DNS debe evitar la consulta DNS a dominios maliciosos.
9.	**ANÁLISIS DE MALWARE MODERNO**
9.1.	Poseer la capacidad de análisis de amenazas no conocidas.
9.2.	Debido a los Malware de hoy en día que son dinámicos, un antivirus común no es capaz de detectar los mismos a la velocidad que sus variaciones son creadas, la solución ofertada deber poseer funcionalidades para análisis de Malware no conocidos incluidas en la propia herramienta. Análisis de malware moderno, que tenga mínimo las siguientes capacidades de análisis: ▪ Análisis estático. ▪ Análisis Dinámico. ▪ Análisis Bare Metal o Anti-VM.
9.3.	El dispositivo de seguridad debe ser capaz de enviar archivos transferidos de forma automática para análisis "In Cloud" o local, donde el archivo será ejecutado y simulado en un ambiente controlado.
9.4.	En caso se trate de sandbox "In Cloud", deberá ser una nube propia del mismo fabricante, con certificación de seguridad y privacidad de datos, como mínimo SOC Tipo 2 o FedRAMP y garantizar un tiempo de análisis de malware de día cero no mayor a 5 minutos.
9.5.	Seleccionar a través de la política de Firewall que tipos de archivos sufrirá este análisis.
9.6.	Soportar el análisis de tipos de comportamientos maliciosos para el análisis de la amenaza no conocida.
9.7.	Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows XP y Windows 7, Windows10.

9.8.	Debe soportar el monitoreo de archivos transferidos por internet (HTTP2, FTP, HTTP, SMTP) como también archivos transferidos internamente en los servidores de archivos usando SMB.
9.9.	El sistema de análisis "In Cloud" o local debe proveer informaciones sobre las acciones del Malware en la máquina infectada, informaciones sobre cuales aplicaciones son utilizadas para causar/propagar la infección, detectar aplicaciones no confiables utilizadas por el Malware, generar firmas de Antivirus y Anti-spyware automáticamente, definir URLs no confiables utilizadas por el nuevo Malware y proveer informaciones sobre el usuario infectado (su dirección IP y su login de red).
9.10.	El sistema automático de análisis "In Cloud" o local debe emitir relación para identificar cuales soluciones de antivirus existentes en el mercado poseen firmas para bloquear el malware.
9.11.	Permitir la carga (subida) de archivos al sandbox de forma manual y vía API.
9.12.	Debe permitir exportar el resultado de los análisis de malware de día Zero en PDF y CSV a partir de la propia interfaz de administración.
9.13.	Debe permitir la descarga de los malware identificados a partir de la propia interfaz de administración.
9.14.	Debe permitir visualizar los resultados de los análisis de malware de día cero[2] en los diferentes sistemas operacionales soportados.
9.15.	Debe permitir informar al fabricante cuando haya una sospecha de falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia interfaz de administración.
9.16.	Soportar el análisis de archivos ejecutables, DLLs, ZIP y encriptados en SSL en el ambiente controlado.
9.17.	Soportar el análisis de archivos en el ambiente controlado de los siguientes tipos: del paquete office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), email, flash, archivos de MacOS (mach-o, dmg, pkg) y Android APKs.
9.18.	Poseer SLA de, como máximo, 5 minutos para actualización de la base de vacunas contra malware desconocidos identificados en el ambiente controlado.
9.19.	Permitir el envío de archivos para análisis en el ambiente controlado vía web y de forma automática vía API.
9.20.	Debe poder dar veredictos distintos del tráfico analizado.
9.21.	En caso de detectar una forma de evasión de máquina virtual, debe poder enviar de forma automática a revisión en modo Bare Metal (maquinas físicas) o el análisis debe ser soportado por la solución de inteligencia de amenazas.
10.	**FILTRO DE URL**
10.1.	La plataforma de seguridad debe poseer las siguientes funcionalidades de filtro de URL
10.2.	Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora).
10.3.	Debe ser posible crear políticas por usuario, grupo de usuario, IPS, redes y zonas de seguridad.
10.4.	Deberá incluir la capacidad de creación de políticas basadas en la visibilidad y contra de quien está utilizando cual URLs a través de la integración con servicios de directorio, autenticación vía LDAP, Active Directory, E-Directory y base de datos local.
10.5.	Debe permitir poder publicar los logs de URL con la información de los usuarios conforme a lo descrito en la integración con servicios de directorio.

[2] Ver funcionalidad descrita en https://es.wikipedia.org/wiki/Ataque_de_d%C3%ADa_cero

10.6.	Incluir funcionalidad de inserción de headers http al menos para Google Gsuite y Microsoft Office365, para diferenciar cuentas corporativas y no corporativas.
10.7.	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría URL.
10.8.	Debe bloquear el acceso a sitios de búsqueda (Google, Bing y Yahoo!) en el caso de que la opción de Safe Search este deshabilitada. Debe en ese caso exhibir una página de bloqueo dando instrucciones al usuario de como habilitar dicha función.
10.9.	Debe soportar una caché local de URL en el appliance, evitando el delay de comunicación/validación de las URLs.
10.10.	Debe poseer al menos 60 categorías de URLs.
10.11.	Debe soportar la creación de categorías URL custom.
10.12.	Debe soportar la exclusión de URLs del bloqueo por categoría.
10.13.	Debe permitir la customización de la página de bloqueo.
10.14.	Debe permitir o bloquear y continuar; habilitando que el usuario con acceso a un sitio potencialmente bloqueado, le informe del bloqueo y le habilite el botón de "continuar" para permitirle seguir a ese sitio si así lo decide.
10.15.	Debe soportar la inclusión de los logs del producto de las informaciones de las actividades de los usuarios.
10.16.	Debe evitar la fuga de credenciales desde o hacia sitios web, pudiendo tener granularidad en la configuración, es decir, poder permitir o no el uso de credenciales de red internas en diferentes categorías de páginas web (estas categorías podrían ser: phishing, redes sociales, foros, o categorías personalizadas por el cliente, etc), en incluso el uso indebido de los mismos dentro de la red del cliente. El objetivo de este requerimiento es evitar que credenciales internas de la red sean publicadas en sitios de internet, inclusive sitios categorizados como desconocidos por el motor de categorización de filtros de URL.
10.17.	Debe poder actualizar de forma automática en cinco (5) minutos o menos las categorías de malware y phishing.
11.	**IDENTIFICACIÓN DE USUARIOS**
11.1.	Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de quien está utilizando cuales aplicaciones a través de la integración como servicios de directorio, autenticación vía ldap, Active Directory, E-directory y base de datos local.
11.2.	Se debe integrar con Microsoft Active Directory de la entidad para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.
11.3.	Debe poseer integración con Radius para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.
11.4.	Debe poseer integración con TACACS+
11.5.	Debe posea integración con Ldap para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en Usuarios y Grupos de usuarios.
11.6.	Debe soportar la recepción de eventos de autenticación de controladoras Wireless, dispositivos 802.1x o soluciones NAC vía syslog, para la identificación de direcciones IP y usuarios.
11.7.	Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal).
11.8.	Soporte a autenticación Kerberos.
11.9.	Soporte SAML 2.0.

11.10.	Debe soportar múltiples factores de autenticación (como por ejemplo usuario y password + 2FA hard token + 2FA soft token + portal cautivo).
11.11.	Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en ambientes Citrix y Microsoft Terminal Server, permitiendo visibilidad y control granular por usuario sobre el uso de las aplicaciones que tiene estos servicios.
11.12.	Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en servidores accedidos remotamente, incluso que no sean servidores Windows.
12.	**QOS**
12.1.	Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube, ustream, etc) y tener un alto consumo de ancho de banda, se requiere que la solución, a la vez de poder permitir o negar ese tipo de aplicaciones, debe tener la capacidad de controlarlas por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones, tanto de audio como de vídeo streaming.
12.2.	Soportar la creación de políticas de QoS por: ▪ Dirección de origen. ▪ Dirección de destino. ▪ Por usuario y grupo de LDAP/AD. ▪ Por aplicaciones, incluyendo, más no limitando a Skype, Bittorrent, YouTube y Azureus; ▪ Por puerto.
12.3.	El QoS debe permitir la definición de clases por: ▪ Ancho de Banda garantizado. ▪ Ancho de Banda Máximo. ▪ Cola de prioridad.
12.4.	Soportar priorización Real Time de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.
12.5.	Soportar marcación de paquetes Diffserv, inclusive por aplicaciones.
12.6.	Disponer de estadísticas Real Time para clases de QoS.
12.7.	Deberá permitir el monitoreo del uso que las aplicaciones hacen por bytes, sesiones y por usuario.
13.	**FILTRO DE DATOS**
13.1.	Permite la creación de filtros para archivos y datos predefinidos.
13.2.	Los archivos deben ser identificados por extensión y firmas.
13.3.	Permite identificar y opcionalmente prevenir la transferencia de varios tipos de archivos (MS Office, PDF, etc) identificados sobre aplicaciones (P2P, InstantMessaging, SMB, etc).
13.4.	Soportar la identificación de archivos compactados y las aplicaciones de políticas sobre el contenido de esos tipos de archivos.
13.5.	Permitir identificar y opcionalmente prevenir la transferencia de informaciones sensibles, incluyendo, más no limitando documentos de las audiencias, permitiendo la creación de nuevos tipos de datos vía expresión regular.
13.6.	Permitir listar el número de aplicaciones soportadas para control de datos.
13.7.	Permitir listar el número de tipos de archivos soportados para el control de datos.
13.8.	Debe poder integrarse son soluciones de punto final de terceros para mejorar la política de DLP. ▪ Identificar el tipo archivo. ▪ Identificar información de tarjetas de crédito.

	▪ información sensible para la Dirección Ejecutiva de la Justicia Penal Militar – MDN.
13.9.	Debe traer por efecto al menos dos perfiles de bloqueo predefinidos.
14.	**GEOLOCALIZACIÓN**
14.1.	Soportar la creación de políticas por Geo-localización, permitiendo que el tráfico de determinado País/Países sean bloqueados.
14.2.	Debe posibilitar la visualización de los países de origen y destino en los logs de acceso.
14.3.	Debe posibilitar la creación de regiones geográficas desde la interfaz gráfica y crear políticas utilizando las mismas.
15.	**VPN**
15.1.	Soportar VPN Site-to-Site y Cliente-To-Site.
15.2.	Soportar IPSec VPN.
15.3.	Soportar SSL VPN.
15.4.	La VPN IPSEc debe soportar: ▪ DES y 3DES; ▪ Autenticación MD5 e SHA-1 o superior. ▪ Diffie-Hellman Group 1, Group 2, Group 5 y Group 14. ▪ Algoritmo Internet Key Exchange (IKEv1 & IKEv2); ▪ AES 128, 192 e 256 (Advanced Encryption Standard). ▪ Debe permitir SSO via Kerberos. ▪ Autenticación via certificado IKE PKI. ▪ Debe ser compatible con la Suite B de protocolos de NSA.
15.5.	Debe poseer interoperabilidad como los siguientes fabricantes: ▪ Cisco. ▪ Checkpoint. ▪ Juniper. ▪ Palo Alto Networks. ▪ Fortinet. ▪ Sonic Wall. ▪ Sophos.
15.6.	Las VPN SSL deben soportar:
15.7.	Permitir que el usuario realice la conexión por medio de cliente instalado en el sistema operacional del equipamiento o por medio de interfaz WEB.
15.8.	Las funcionalidades de VPN SSL deben ser atendidas con o sin el uso de agente.
15.9.	La asignación de dirección IP en los clientes remotos de VPN.
15.10.	La asignación de DNS en los clientes remotos de VPN.
15.11.	Debe haber la opción de ocultar el agente de VPN instalado en el cliente remoto, tornando el mismo invisible para el usuario.
15.12.	Deber permitir crear políticas de control de aplicaciones, IPS, Antivirus, Antispyware para tráfico de los clientes remotos conectados en la VPN SSL.
15.13.	Las VPN SSL deben soportar proxy arp y el uso de interfaces PPPOE.
15.14.	Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.
15.15.	Permite establecer un túnel VPN client-to-site del cliente a la plataforma de seguridad, proveyendo una solución de single-sign-on a los usuarios, integrándose como las herramientas de Windows-logon.
15.16.	Soporte de lectura y verificación de CRL (certificate revocation list).
15.17.	Permite la aplicación de políticas de seguridad y visibilidades para las aplicaciones que circulan dentro de los túneles SSL.

15.18.	El agente de VPN a ser instalado en los equipamientos desktop y laptops, debe ser capaz de ser distribuido de manera automática vía Microsoft SMS, Active Directory y ser descargado directamente desde su propio portal, en el cual residirá el centralizador de VPN.
15.19.	El agente deberá comunicarse con el portal para determinar las políticas de seguridad del usuario.
15.20.	Debe permitir que las conexiones como VPN SSL sean establecidas de las siguientes formas:
15.21.	Antes del usuario autenticarse en la estación.
15.22.	Después de la autenticación del usuario en la estación.
15.23.	Bajo demanda del usuario.
15.24.	Deberá mantener una conexión segura con el portal durante la sesión.
15.25.	El agente de VPN SSL client-to-site debe ser compatible al menos con: Windows XP, Vista, Windows 7, Windows 8, Windows 10, MacOS X.
15.26.	El portal de VPN debe enviar al cliente remoto la lista de gateways VPN activos para el establecimiento de la conexión, los cuales deben poder ser administrados centralizadamente.
15.27.	Debe haber una opción en el cliente remoto de escoger manualmente el Gateway de VPN y de forma automática a través de la mejor respuesta entre los gateways disponibles con base al más rápido.
15.28.	Debe poseer la capacidad de identificar el origen de conexión de VPN si es interna o externa.
16.	**CONSOLA DE ADMINISTRACIÓN Y MONITOREO**
16.1.	La administración de la solución debe soportar acceso vía SSH, cliente WEB (HTTPS) y API abierta.
16.2.	En el caso de que sea necesaria la instalación de cliente para administración de la solución, el mismo debe ser compatible con sistemas operacionales Windows y Linux.
16.3.	La administración debe permitir/hacer:
16.4.	Creación y administración de políticas de firewall y control de aplicaciones.
16.5.	Creación y administración de políticas de IPS y Anti-Spyware.
16.6.	Creación y administración de políticas de filtro de URL.
16.7.	Monitoreo de logs.
16.8.	Herramientas de investigación de logs.
16.9.	Debugging.
16.10.	Captura de paquetes.
16.11.	Debe permitir el acceso concurrente de administradores.
16.12.	Debe tener un mecanismo de búsqueda de comandos de administración vía SSH, facilitando la localización de los comandos.
16.13.	Debe permitir usar palabras clave y distintos tags de colores para facilitar la identificación de Reglas.
16.14.	Debe permitir monitorear vía SNMP fallas en el hardware, inserción o remoción de fuentes, discos y ventiladores, uso de recursos por número elevado de sesiones, número de túneles establecidos de VPN cliente-to-site, porcentaje de utilización en referencia al número total soportado/licenciado y número de sesiones establecidas.
16.15.	Debe permitir el bloqueo de alteraciones, en el caso de acceso simultaneo de dos o más administradores.
16.16.	Debe permitir la definición de perfiles de acceso a la consola con permisos granulares como: acceso de escritura, acceso de lectura, creación de usuarios, alteración de configuraciones.

16.17.	Debe permitir la autenticación integrada con Microsoft Active Directory y servidor Radius.
16.18.	Debe permitir la localización de donde están siendo utilizados objetos en: Reglas, dirección IP, Rango de IPs, subredes u objetos.
16.19.	Debe poder atribuir secuencialmente un número a cada regla de firewall, NAT, QOS y Reglas de DOS.
16.20.	Debe permitir la creación de Reglas que estén activas en un horario definido.
16.21.	Debe permitir la creación de Reglas con fecha de expiración.
16.22.	Debe poder realizar un backup de las configuraciones y rollback de configuración para la última configuración salvada.
16.23.	Debe soportar el Rollback de Sistema operativo para la última versión local.
16.24.	Debe poseer la habilidad del upgrade vía SCP, TFTP e interfaz de administración.
16.25.	Debe poder validar las Reglas antes de las aplicaciones.
16.26.	Debe permitir la validación de las políticas, avisando cuando haya Reglas que ofusquen o tengan conflicto con otras (shadowing).
16.27.	Debe posibilitar la visualización y comparación de configuraciones actuales, la configuración anterior y configuraciones más antiguas.
16.28.	Debe posibilitar la integración con otras soluciones de SIEM del mercado (third-party SIEM vendors).
16.29.	Debe permitirá la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizo y el horario de la alteración.
16.30.	Deberá tener la capacidad de generar un gráfico que permita visualizar los cambios en la utilización de aplicaciones en la red en lo que se refiere a un periodo de tiempo anterior, para permitir comparar los diferentes consumos realizados por las aplicaciones en el tiempo presente con relación al pasado.
16.31.	Debe permitir la generación de mapas geográficos en tiempo real para la visualización de orígenes y destinos del tráfico generado en la institución.
16.32.	Debe proveer resúmenes con la vista correlacionada de aplicaciones, amenazas (IPS, Antispyware) URLs y filtro de archivos, para un mejor diagnóstico y respuesta a incidentes.
16.33.	Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información con base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.
16.34.	La administración de la solución debe posibilitar la recolección de estadísticas de todo el tráfico que pasa por los dispositivos de seguridad.
16.35.	Debe proveer resúmenes de utilización de los recursos por aplicaciones, amenazas (IPS, Anti-Spyware y antivirus de la solución), etc.
16.36.	Debe proveer de una visualización sumarizada de todas las aplicaciones, amenazas (IPS, Antivirus e Anti-Spyware) y URLs que pasan por la solución.
16.37.	Debe poseer un mecanismo "Drill-Down" para navegación por los resúmenes en tiempo real.
16.38.	En las listas de "Drill-Down", debe ser posible identificar el usuario que ha determinado el acceso.
16.39.	Debe ser posible exportar los logs en CSV.
16.40.	Deberá ser posible acceder al equipamiento a aplicar configuraciones durante momentos donde el tráfico sea muy alto y la CPU y memoria del equipamiento este siendo totalmente utilizada.
16.41.	Debe tener rotación de logs.

16.42.	Debe tener presentaciones de las siguientes informaciones, de forma histórica y en tiempo real (actualizado de forma automática y continua cada 1 minuto):
16.43.	Debe mostrar la situación del dispositivo y del cluster.
16.44.	Debe poder mostrar las principales aplicaciones.
16.45.	Debe poder mostrar las principales aplicaciones por riesgo.
16.46.	Debe poder mostrar los administradores autenticados en la plataforma de seguridad.
16.47.	Debe poder mostrar el número de sesiones simultáneas.
16.48.	Debe poder mostrar el estado de las interfaces.
16.49.	Debe poder mostrar el uso de CPU.
16.50.	Generación de reportes. Como mínimo los siguientes reportes deben poder ser generados.
16.51.	Resumen gráfico de las aplicaciones utilizadas.
16.52.	Principales aplicaciones por utilización de ancho de banda de entrada y salida.
16.53.	Principales aplicaciones por tasa de transferencia en bytes.
16.54.	Principales hosts por número de amenazas identificadas.
16.55.	Actividades de un usuario especifico y grupo de usuarios del AD/LDAP, incluyendo aplicaciones accedidas y amenazas (IPS, y Anti-Spyware), de red vinculadas a este tráfico.
16.56.	Debe permitir la creación de reportes personalizados; permitiendo mostrar información de eventos de antivirus, antispyware, IPS, navegación a internet, aplicaciones, malware de dia cero, debe permitir seleccionar las columnas a mostrar, filtrar la información con base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente via correo electrónico.
16.57.	En cada criterio de búsqueda del log debe ser posible incluir múltiples entradas (ej. 10 redes e IP's distintas; servicios HTTP, HTTPS y SMTP), excepto en el campo horario, donde debe ser posible definir un rango de tiempo como criterio de búsqueda.
16.58.	Generar alertas automáticas vía: ▪ Email. ▪ SNMP. ▪ Syslog.
16.59.	El equipo deberá soportar el envio de logs a un servidor externo syslog según RFC 3164.
16.60.	La plataforma de seguridad debe permitir a través de API-XML (Application Program Interface) la integración con sistemas existentes en el ambiente de producción, de forma que posibilite que aplicaciones desarrolladas por el cliente puedan interactuar en tiempo real con la solución permitiendo asi que Reglas y políticas de seguridad puedan ser modificadas por estas aplicaciones con la utilización de scripts en lenguajes de programación como Perl o PHP.
16.61.	Las reglas establecidas en una política de seguridad individual deben determinar si bloquea o permite una sesión en función de los atributos de tráfico, como la zona de seguridad de origen y destino, dirección IP de origen y destino, aplicación, usuario y el servicio.
16.62.	El fabricante deberá permitir realizar auditoria a los cambios de configuración y políticas de seguridad.
16.63.	La consola de administración debe permitir al administrador o administradores, configurar las políticas de seguridad en una única regla, con los siguientes campos: ▪ Nombre de la política o regla.

	▪ Origen: basado en dirección IP, grupos, redes y/o Usuarios o grupo de usuarios del AD. ▪ Destino: basado en dirección IP, grupos, redes y/o Usuarios o grupo de usuarios del AD. ▪ Servicio/aplicación: Protocolo, puerto, aplicación y/o sitio Web (URL, dominio). ▪ Datos: Identificación del tipo de dato, archivo o información, en caso de que aplique para evitar la fuga de información. ▪ Horario: Poder definir los días o lapsos horarios en los que la regla puede operar o la fecha de expiración de la misma. ▪ Acción: Aceptar, rechazar, denegar. ▪ Registros: Indicar si se desea almacenar el registro del tráfico que hace match por la regla o no. ▪ Comentarios: Campo para documentar la política. Se debe manejar un único set de políticas para IPv4 e IPv6.
16.64.	La consola de administración deberá contar con la funcionalidad de creación rápida de reacción por actividad sospechosa, sin necesidad de modificar todo el set de políticas de seguridad.
16.65.	La solución debe poseer una vista de todas las aplicaciones que maneja con una calificación en nivel de riesgo recomendada, que le permita al administrador tomar decisiones al momento de crear las políticas de acceso o bloqueo.
16.66.	La consola de administración y monitoreo puede residir en el mismo appliance de seguridad de red, desde que posea recurso de CPU, memoria, interfaz de red y sistema operacional dedicados para esta función; en caso de no cumplir con esta condición, se deberá asignar un appliance dedicado a esta funcionalidad.
16.67.	La administración de la solución debe posibilitar un conjunto de estadísticas de todo el tráfico que pasa por los equipos de la plataforma de seguridad.
16.68.	El appliance debe tener la capacidad de consolidar logs y reportes de la solución misma de seguridad.
16.69.	Debe permitir exportar backups de configuración automáticamente vía programación.
16.70.	Debe permitir realizar RBAC (Rol based administration) desde el directorio activo.
17.	**SERVICIOS**
17.1.	El oferente deberá realizar el levantamiento de información en detalle de la plataforma actual de marca checkpoint comprendida por los siguientes elementos: ▪ Dos (02) firewall NGFW 4800 versión R77.30. ▪ Un (01) Management virtual open server versión R80.20. ▪ Un (01) eventia report virtual open server versión R80.20. Se recalca que dentro de las actividades de migración e implementación se deberán conservar las reglas existentes de filtrado para las redes utilizadas por la Entidad.
17.2.	El Equipo de trabajo de **USCOM S.A.S.**, debe estar conformado por: a) Gerente de proyecto, debe ser ingeniero o administrador con certificación en administración de proyectos o con certificación PMI vigente a la fecha del cierre del presente proceso de selección y experiencia profesional de mínimo dos (2) años en migración de Firewalls. b) Un ingeniero con certificación del fabricante como profesional en seguridad de redes o un ingeniero que haya cursado y aprobado el 100% de la especialización en seguridad informática, vigente a la fecha del cierre del presente proceso de selección y con mínimo dos (2) años de experiencia específica en migración de Firewalls de la marca ofrecida en la solución.

	c) Un técnico, tecnólogo o ingeniero en instalación de firewall con mínimo dos (2) años de experiencia en la instalación, eléctrica y de redes de Firewalls ofrecidos. **USCOM S.A.S.**, debe hacer llegar las hojas de vida al supervisor, cinco (5) días siguientes a la firma del acta de inicio del contrato.
17.3.	La migración de comprender:
17.3.1.	Realizar una revisión física y análisis de redes y seguridad en el centro de datos (Data Center) ubicado carrera 54 No. 26-25 primer piso Ministerio de Defensa Nacional en la ciudad de Bogotá D.C. con el propósito de evidenciar las condiciones eléctricas, ambientales y físicas generales requeridas para la instalación de los equipos ofertados que se deben instalar y configurar.
17.3.2.	Validar la configuración actual de la plataforma y realizar los backups necesarios antes de realizar algún ajuste o cambio con posibilidad de realizar un roll back en caso de ser necesario
17.3.3.	Realizar la planeación de las actividades en Microsoft Project, las cuales serán presentadas al supervisor del contrato que designe la Dirección Ejecutiva de la Justicia Penal Militar – MDN para la aprobación e inicio de las mismas.
17.3.4.	Suministrar, instalar, configurar, y entregar en correcto funcionamiento la solución de Firewall NGFW en alta disponibilidad, integrada a la red de la entidad en los segmentos de LAN, DMZ, internet y canales privados entre sedes.
17.3.5.	Realizar las configuraciones necesarias a nivel de los segmentos de red, enrutamiento y seguridad en la red de la entidad, de común acuerdo con los administradores del área de Tecnología programando los cambios necesarios para no afectar el servicio en los tiempos que se definan de común acuerdo con la Dirección Ejecutiva de la Justicia Penal Militar –MDN.
17.3.6.	Realizar la configuración de las VPNs para trabajo en casa de mínimo setenta (70) funcionarios de la entidad con su respectiva documentación, sensibilización y ajustes que sean solicitados por el supervisor del Contrato.
17.3.7.	Entregar la documentación pertinente a la configuración de la solución y escalamiento de incidentes.
17.4.	Servicio de soporte de fábrica:
17.4.1.	Soporte de primer nivel y segundo nivel durante la ejecución del contrato.
17.4.2.	Como parte de la garantía, realizar mínimo dos (2) visitas durante la vigencia del soporte, en las instalaciones de la Dirección Ejecutiva de la Justicia Penal Militar –MDN, para diagnóstico y afinamiento de la solución objeto de la presente contratación. Se debe suministrar un reporte escrito de cada visita, efectuando los ajustes que se requieran como resultado del diagnóstico y consignando recomendaciones para obtener el mejor desempeño de la solución del Firewall.
17.4.3.	Escalar con el fabricante de ser necesario el reemplazo de piezas y actuaciones en sitio. El reemplazo de piezas se hará por procedimiento de RMA.
17.4.4.	Las actualizaciones de software o firmware solo serán realizadas por recomendación del fabricante para la solución de un incidente durante la vigencia contrato.
17.5.	El oferente entregará una Bolsa de 192 horas de asistencia en sitio y/o remoto para la administración de la solución, resolución de ataques, fallos incidentes o problemas que afecten la solución, que no incluye el soporte del fabricante.
17.5.1.	Servicio en sitio prestado con personal propio de **USCOM S.A.S.**, certificado por el fabricante de la solución.
17.5.2.	Gestión de las incidencias, diagnóstico y resolución en remoto y en sitio durante la ejecución del contrato, de ser necesario deberá ser escalado ante el fabricante.
18.	**CUMPLIMIENTOS LEGALES**

18.1.	Dada la naturaleza de las actividades a realizar en desarrollo del objeto contractual, se debe garantizar la integridad y confidencialidad de la información institucional a la cual llegue a tener acceso directamente o por intermedio de terceros, para lo cual **USCOM S.A.S.**, suscribe el respectivo compromiso de confidencialidad que hará parte integral del contrato.
18.2.	De igual manera, el diseño, las pruebas y sus resultados, las políticas y los procesos en la actualización de la solución serán considerados por **USCOM S.A.S.**, como información confidencial propiedad de la Dirección Ejecutiva de la Justicia Penal Militar - MDN, en tal virtud, adoptará todas las medidas necesarias para impedir su duplicación, sustracción, divulgación, alteración, ocultamiento o utilización indebida.
18.3.	Durante el diseño, pruebas, actualización y soporte de la solución, **USCOM S.A.S.**, se compromete a no hacer uso indebido de las herramientas utilizadas en desarrollo del objeto contractual, ni duplicar, sustraer, divulgar o alterar información a la cual pueda tener acceso a través de ellas.
18.4.	**USCOM S.A.S.**, deberá cumplir con los derechos de autor, con el fin de que la Dirección Ejecutiva de la Justicia Penal Militar–MDN quede indemne ante cualquier reclamación por parte de los dueños de dichos derechos que se utilicen en la suscripción al servicio en la nube y en el software de los equipos que conforman la solución del Firewall contratada.

16 DIC. 2020

OTTO FRANCISCO URREA JARAMILLO
Representante Legal de **USCOM S.A.S.**

PD. Fredy Arbey Romero Silva-Estructurador Técnico
Ing. Luis Alirio Dorado Bravo - Evaluador Técnico

ANEXO No. 2
COMPROMISO CONFIDENCIALIDAD DEL CONTRATO

Que libre y voluntariamente, de manera unilateral, en mí propio nombre y de los empleados o asesores que se vinculen a la empresa que represento para efectos de ejecución del presente contrato, asumo el presente COMPROMISO DE CONFIDENCIALIDAD, teniendo en cuenta las siguientes consideraciones:

PRIMERA: Que la **DIRECCIÓN EJECUTIVA JUSTICIA PENAL MILITAR – MDN,** adelantó el Proceso de Selección Abreviada – Subasta Inversa Electrónica No. 043-2020 DEJPM-MDN, cuyo objeto es: Adquisición de equipos de seguridad perimetral firewall para la Dirección Ejecutiva de la Justicia Penal Militar - MDN incluido licenciamiento, soporte en sitio requerido y mantenimiento de conformidad con las especificaciones técnicas mínimas exigidas

SEGUNDA: Que es mi propósito apoyar la gestión de la institución en lo que hace a la apertura y democratización de los procesos, sobre esquemas fortalecidos hacia la transparencia en los procesos de contratación, la garantía de información objetiva y la confidencialidad.

TERCERA: Que siendo de interés en mi propio nombre, me encuentro dispuesto a asumir con la debida confidencialidad la información propia de la ejecución del contrato; en tal sentido suscribo el presente documento de confidencialidad por el cual se garantiza absoluta reserva sobre la información y lugares de la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MDN** a los cuales tenga acceso.

CUARTA: Que por tanto, asumo libre y espontáneamente este compromiso, el cual se regirá por las siguientes cláusulas:

CLÁUSULA PRIMERA COMPROMISO ASUMIDO POR USCOM S.A.S.: Mediante la suscripción del presente documento, asumo el siguiente compromiso:

USCOM S.A.S., se compromete formalmente a impartir instrucciones a todos sus empleados, agentes, asesores, y a cualquier otro representante suyo, exigiéndoles el cumplimiento en todo momento de las leyes de la República de Colombia, especialmente de aquellas que rigen la presente relación contractual, y les pondrá las obligaciones de:

a) No revelar información propia de la **DIRECCIÓN EJECUTA DE LA JUSTICIA PENAL MILITAR-MDN**, ni sobre los lugares a los cuales tenga acceso, con ocasión de la ejecución del presente contrato.
b) No permitir que terceros obtengan información relacionada con el literal anterior.
c) No obrar a través de terceros o sugerir que terceros hagan lo propio en su nombre.

d) No publicar información alguna, por medios de comunicación electrónica o correos internos de su grupo empresarial, que permita a terceros o a sus funcionarios no autorizados acceder a la información.

CLÁUSULA SEGUNDA. CONSECUENCIAS DE INCUMPLIMIENTO: USCOM S.A.S., asume a través de la suscripción del presente compromiso, las consecuencias que la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MDN** considere procedente imponer, entre ellas, la presentación pública de su conducta trasgresora; igualmente, si la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR - MDN** demuestra que con su actuación se vulneran los derechos, podrá ejercer las acciones civiles, penales y administrativas que le permitan restablecer su situación, previa indemnización del daño causado.

CLÁUSULA TERCERA: Declara igualmente **USCOM S.A.S.**, que toda la información que se produzca en la ejecución del contrato, será confidencial y/o reservada.

En constancia de lo anterior, y como manifestación de la aceptación de los compromisos unilaterales incorporados en el presente documento, se firma el mismo en la ciudad de Bogotá D.C., a los 16 DIC. 2020

OTTO FRANCISCO URREA JARAMILLO
Representante Legal de **USCOM S.A.S.**

ANEXO No. 3
CLÁUSULA CONTRACTUAL DE CATALOGACIÓN

De conformidad con lo establecido en el Contrato de Compraventa No. 043-2020 DEJPM-MDN de_____ cuyo objeto es: *"Adquisición de equipos de seguridad perimetral firewall para la Dirección Ejecutiva de la Justicia Penal Militar - MDN incluido licenciamiento, soporte en sitio requerido y mantenimiento de conformidad con las especificaciones técnicas mínimas exigidas"*, **USCOM S.A.S.**, deberá proporcionar **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MD** una lista de los bienes adjudicados, con la información técnica necesaria para la identificación de los artículos de abastecimiento incluidos en el objeto del contrato así:

Información del contratista.

Dirección _____
Nombre de la empresa_____
Teléfono._____
Correo electrónico_____
Código de identificación tributaria._____
País de origen._____

Información del fabricante del artículo de abastecimiento.

Dirección _____
Nombre de la empresa_____
Teléfono_____
Correo electrónico_____
Código de identificación tributaria_____
País de origen._____

Datos técnicos a suministrar del artículo de abastecimiento.

Nombre técnico del artículo asignado por el fabricante.____
Número de pieza o referencia._____
Número OTAN ó National Stock Number._____
Especificaciones y documentación técnica **emitida por el Fabricante.**
Planos de ingeniería. ☐
Dibujos técnicos. ☐
Manual del fabricante ☐
Fichas técnicas ☐
Catálogo de partes ☐

A los efectos anteriores, **USCOM S.A.S.**, será responsable de obtener de sus subcontratistas o proveedores, los datos técnicos necesarios para la identificación del artículo de fabricación nacional, de un país no OTAN o un país no apadrinado por la OTAN.

En caso de que el artículo procedan de un país OTAN o apadrinado nivel (Tier) 2, **USCOM S.A.S.**, deberá suministrar el número OTAN de Catalogo (NOC), relacionado con el artículo objeto del contrato. Si el artículo no está catalogado, **USCOM S.A.S.** deberá presentar la certificación de que se encuentra en trámite de catalogación.

USCOM S.A.S., acreditará el cumplimiento de la cláusula de catalogación, mediante un certificado expedido por la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN** el cual certificará la entrega total de la información de acuerdo a los lineamientos establecidos en el presente anexo, por el Grupo de Catalogación de Defensa y el contrato.

USCOM S.A.S., acreditará el cumplimiento de la cláusula de catalogación, mediante un certificado expedido por la **DIRECCIÓN EJECUTIVA DE LA JUSTICIA PENAL MILITAR – MDN**, el cual certificará la entrega total de la información de acuerdo a los lineamientos establecidos por el Grupo de Catalogación de Defensa y en el contrato.

EL CONTRATISTA,

OTTO FRANCISCO URREA JARAMILLO
Representante Legal de **USCOM S.A.S.**