CONTRATO DE ARRENDAMIENTO SIN OPCIÓN A COMPRA QUE CELEBRAN POR UNA PARTE EL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, A QUIÉN EN LO SUCESIVO SE LE DENOMINARÁ "INAI", REPRESENTADO EN ESTE ACTO POR EL LIC. RAFAEL ESTRADA CABRAL, EN SU CARÁCTER DE APODERADO LEGAL, CON LA ASISTENCIA DEL ING. JOSÉ LUIS HERNÁNDEZ SANTANA, DIRECTOR GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN; Y POR LA OTRA GRUPO DE TECNOLOGÍA CEBERNÉTICA, S.A. DE C.V., A QUIÉN EN LO SUCESIVO SE LE DENOMINARÁ "PROVEEDOR" REPRESENTADA EN ESTE ACTO POR SELENE ELIZABETH CASTAÑON GUTIERREZ EN SU CARÁCTER DE REPRESENTANTE LEGAL DE CONFORMIDAD CON LAS SIGUIENTES DECLARACIONES Y CLÁUSULAS:

D E C L A R A C I O N E S

I.- EL "INAI" DECLARA:

I.1.- SER UN ORGANISMO AUTÓNOMO EN TERMINOS DE LO DISPUESTO EN EL ARTICULO 6º APARTADO A FRACCIÓN VIII DE LA CONSTITUCIÓN POLITICA DE LOS ESTADOS UNIDOS MEXICANOS, RESPONSABLE DE GARANTIZAR EL CUMPLIMIENTO DEL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA Y A LA PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS SUJETOS OBLIGADOS, DE CONFORMIDAD CON EL DECRETO POR EL QUE SE REFORMAN Y ADICIONAN DIVERSAS DISPOSICIONES DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, EN MATERIA DE TRANSPARENCIA", PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 07 DE FEBRERO DE 2014.

I.2.- QUE EN VIRTUD DE LA PUBLICACIÓN DEL DECRETO POR EL QUE SE EXPIDE LA LEY GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA EL 04 DE MAYO DE 2015 EN EL DIARIO OFICIAL DE LA FEDERACIÓN, ESTE ORGANISMO AUTÓNOMO SE DENOMINA INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES.

I.3.- QUE EL LIC. RAFAEL ESTRADA CABRAL, EN SU CARÁCTER DE APODERADO LEGAL, FIRMA EL PRESENTE CONTRATO DE CONFORMIDAD CON LAS FACULTADES LEGALES CONSIGNADAS EN EL INSTRUMENTO NÚMERO 125,318 DE FECHA 19 DE AGOSTO DE 2019, PASADO ANTE LA FE DEL LIC. ALFONSO ZERMEÑO INFANTE TITULAR DE LA NOTARIA NÚMERO 5 DE LA CIUDAD DE MÉXICO, LAS CUÁLES NO LE HAN SIDO REVOCADAS NI MODIFICADAS EN FORMA ALGUNA A LA FECHA.

I.4.- DE CONFORMIDAD CON EL CAPITULO X NUMERAL 5 PENÚLTIMO PÁRRAFO DE LAS BASES Y LINEAMIENTOS EN MATERIA DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, EN LO SUCESIVO "BALINES" Y AL ARTÍCULO 48 DEL ESTATUTO ÓRGANICO DEL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL DÍA 17 DE ENERO DE 2017, EL ING. JOSÉ LUIS HERNÁNDEZ SANTANA DIRECTOR GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN, ÁREA REQUIRENTE, ES EL SERVIDOR PÚBLICO RESPONSABLE DE ADMINISTRAR Y VIGILAR LA CONTRATACIÓN Y DE DAR CUMPLIMIENTO A LAS OBLIGACIONES QUE SE DERIVEN DEL OBJETO DEL PRESENTE CONTRATO, EN EL ÁMBITO DE SU COMPETENCIA.

I.5.- QUE PARA CUMPLIR CON LOS PROGRAMAS Y SERVICIOS QUE TIENE LEGALMENTE ENCOMENDADOS, REQUIERE LA CONTRATACIÓN DEL "ARRENDAMIENTO SIN OPCIÓN A COMPRA DE UNA SOLUCIÓN DE SEGURIDAD PERIMETRAL".

I.6.- QUE PARA CUBRIR LAS EROGACIONES QUE SE DERIVEN DEL PRESENTE CONTRATO, CUENTA CON LOS RECURSOS PRESUPUESTARIOS SUFICIENTES EN LA PARTIDA NÚMERO 32301 CORRESPONDIENTE AL CLASIFICADOR POR OBJETO DEL GASTO PARA LA ADMINISTRACIÓN PUBLICA

REVISADO - DEPARTAMENTO LEGAL - GRUPOTECNO

FEDERAL, CUYA ÚLTIMA MODIFICACIÓN FUE PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 26 DE JUNIO DE 2018 EN TÉRMINOS DE LO SEÑALADO EN LA RESERVA PRESUPUESTAL NUMERO 441/802 EMITIDA POR EL SISTEMA DE CONTROL DE DISPONIBILIDADES DEL "INAI".

I.7.- QUE MEDIANTE ACUERDO DEL PLENO DEL **"INAI"** NÚMERO ACT-PUB/21/08/2019.08 AUTORIZA LA CONTRATACIÓN PLURIANUAL POR 36 MESES DEL ARRENDAMIENTO DEL PRESENTE INSTRUMENTO.

I.8.- QUE LA ADJUDICACIÓN DEL PRESENTE CONTRATO SE REALIZÓ MEDIANTE EL PROCEDIMIENTO DE **LICITACIÓN PÚBLICA DE CARÁCTER INTERNACIONAL ABIERTA CON NÚMERO DE CLAVE INTERNA LPIA-006HHE001-020-19 Y CON CLAVE ELECTRÓNICA LA-006HHE001-E78-2019** CONFORME A LO DISPUESTO POR LOS ARTICULOS 26, FRACCIÓN I, 28 FRACCIÓN I Y 47, DEL REGLAMENTO DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, EN LO SUCESIVO "RAAS".

I.9.- QUE SU CLAVE DEL REGISTRO FEDERAL DE CONTRIBUYENTES ES **INA1402082Z8**.

I.10.- QUE, PARA EL EJERCICIO Y CUMPLIMIENTO DE LOS DERECHOS Y OBLIGACIONES A SU CARGO, QUE SE DERIVEN DEL PRESENTE INSTRUMENTO, SEÑALA COMO DOMICILIO LEGAL EL UBICADO EN AVENIDA INSURGENTES SUR 3211, COLONIA INSURGENTES CUICUILCO, ALCALDÍA COYOACÁN, C.P. 04530, CIUDAD DE MÉXICO.

II. EL "PROVEEDOR" DECLARA:

II.1.- QUE ES UNA SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE DE NACIONALIDAD MEXICANA CONSTITUIDA CONFORME A LAS LEYES MEXICANAS, LO CUAL ACREDITA CON TESTIMONIO DE LA ESCRITURA PÚBLICA NÚMERO 88,838 (OCHENTA Y OCHO MIL OCHOCIENTOS TREINTA Y OCHO) DE FECHA 17 DE ABRIL DE 1998, ANTE LA FE PÚBLICA DE JOSÉ ÁNGEL VILLALOBOS MAGAÑA, TITULAR DE LA NOTARÍA PÚBLICA NÚMERO 9, QUEDANDO DEBIDAMENTE INSCRITA EN EL REGISTRO PUBLICO DE LA PROPIEDAD Y DEL COMERCIO DEL ENTONCES DISTRITO FEDERAL EL DÍA 4 DE MAYO DE 1998.

MEDIANTE LAS POLIZAS NÚMEROS 34,082 (TREINTA Y CUATRO MIL OCHENTA Y DOS) DE FECHA 22 DE DICIEMBRE DE 2014, 35,405 (TREINTA Y CINCO MIL CUATROCIENTOS CINCO) DE FECHA 9 DE JUNIO DE 2015 Y 41,898 (CUARENTA Y UN MIL OCHOCIENTOS NOVENTA Y OCHO) DE FECHA 12 DE JULIO DE 2017 TODAS ANTE LA FE PÚBLICA DEL LICENCIADO JUAN MARTÍN ÁLVAREZ MORENO CORREDOR PÚBLICO NÚMERO 46 DEL ENTONCES DISTRITO FEDERAL DONDE SE APROBÓ EL AUMENTO DEL CAPITAL SOCIAL.

MEDIANTE LA ESCRITURA PÚBLICA NÚMERO 61, 287 (SESENTA Y UN MIL DOSCIENTOS OCHENTA Y SIETE) DE FECHA 17 DE DICIEMBRE DE 2018, ANTE LA FE PÚBLICA DE EMILIANO ZUBIRÍA MAQUEO, TITULAR DE LA NOTARÍA PÚBLICA NÚMERO 25 DE LA CIUDAD DE MÉXICO, SE AUTORIZA LA VENTA DE ACCIONES DE LA SOCIEDAD DEL SEÑOR MARIO JOSÉ SAUZA DONES.

II.2.- QUE SU REPRESENTANTE LEGAL, C **SELENE ELIZABETH CASTAÑON GUTIERREZ**, CUENTA CON FACULTADES SUFICIENTES PARA LA CELEBRACIÓN DEL PRESENTE INSTRUMENTO, LO CUAL ACREDITA MEDIANTE ESCRITURA PÚBLICA NÚMERO 60,340 (SESENTA MIL TRESCIENTOS CUARENTA) DEL 7 DE FEBRERO DE 2018, PASADA ANTE LA FE DEL LICENCIADO EMILIANO ZUBIRÍA MAQUEO, TITULAR DE LA NOTARÍA NÚMERO 25 DE LA CIUDAD DE MÉXICO, ASIMISMO DECLARA QUE DICHAS FACULTADES NO LE HAN SIDO REVOCADAS, NI MODIFICADAS EN FORMA ALGUNA.

REVISADO - DEPARTAMENTO LEGAL - GRUPOTECNO

II.3.- QUE HA CONSIDERADO TODOS LOS FACTORES QUE INTERVIENEN EN LA EJECUCIÓN, DE LA PRESTACIÓN DEL SERVICIO CONTRATADO, ASÍ COMO LAS ESPECIFICACIONES CONTENIDAS EN EL ANEXO TÉCNICO DE ESTE INSTRUMENTO.

II.4.- QUE REÚNE LA CAPACIDAD TÉCNICA Y LOS ELEMENTOS PROPIOS Y SUFICIENTES PARA OBLIGARSE A LA EJECUCIÓN DE LA PRESTACIÓN DEL ARRENDAMIENTO CONTRATADO, OBJETO DEL PRESENTE CONTRATO.

II.5- BAJO PROTESTA DE DECIR VERDAD, QUE NO SE ENCUENTRA EN NINGUNO DE LOS SUPUESTOS CONTENIDOS EN LOS ARTICULOS 49 Y 63 DEL RAAS.

II.6.- MANIFIESTA QUE SE ENCUENTRA AL CORRIENTE EN EL CUMPLIMIENTO DE SUS OBLIGACIONES FISCALES, DE CONFORMIDAD CON LAS DISPOSICIONES DEL CÓDIGO FISCAL DE LA FEDERACIÓN Y LAS LEYES TRIBUTARIAS VIGENTES.

II.7.- QUE DE CONFORMIDAD CON LO SEÑALADO EN EL ARTÍCULO 3º FRACCIÓN III DE LA LEY PARA EL DESARROLLO DE LA COMPETITIVIDAD DE LA MICRO, PEQUEÑA Y MEDIANA EMPRESA, SE ESTRATIFICA COMO UNA EMPRESA GRANDE.

II.8.- QUE EN CUMPLIMIENTO AL ACUERDO POR EL QUE SE CREA CON CARÁCTER PERMANENTE LA COMISIÓN INTERSECRETARIAL DE COMPRAS Y OBRAS DE LA ADMINISTRACIÓN PÚBLICA FEDERAL A LA MICRO, PEQUEÑA Y MEDIANA EMPRESA, SE COMPROMETE A INSCRIBIRSE EN EL DIRECTORIO DE PROVEEDORES DEL GOBIERNO FEDERAL DE NACIONAL FINANCIERA, SOCIEDAD NACIONAL DE CRÉDITO, INSTITUCIÓN DE BANCA DE DESARROLLO.

II.9.- QUE SU CLAVE DEL REGISTRO FEDERAL DE CONTRIBUYENTES ES **GTC980421R4A**.

II.10.- QUE PARA EL EJERCICIO Y CUMPLIMIENTO DE LOS DERECHOS Y OBLIGACIONES QUE SE DERIVAN DEL PRESENTE CONTRATO SEÑALA COMO SU DOMICILIO LEGAL EL UBICADO EN CALLE REVOLUCIÓN 1145, COLONIA MERCED GÓMEZ, ALCALDÍA BENITO JUÁREZ, CÓDIGO POSTAL 03930, CIUDAD DE MÉXICO.

HECHAS LAS DECLARACIONES QUE ANTECEDEN LAS PARTES CONVIENEN EN OBLIGARSE Y CONTRATAR AL TENOR DE LAS SIGUIENTES:

C L Á U S U L A S

PRIMERA. OBJETO

EL **"INAI"** ENCOMIENDA AL **"PROVEEDOR"** EL "ARRENDAMIENTO SIN OPCIÓN A COMPRA DE UNA SOLUCIÓN DE SEGURIDAD PERIMETRAL" EN LOS TÉRMINOS PACTADOS EN EL PRESENTE INSTRUMENTO Y CONFORME A LAS MODALIDADES, ESPECIFICACIONES Y CARACTERÍSTICAS CONTENIDAS EN EL ANEXO TÉCNICO.

SEGUNDA. RELACIÓN DE ANEXOS

ES PARTE INTEGRANTE DE ESTE CONTRATO EL ANEXO TÉCNICO EL CÚAL ES ABSOLUTA RESPONSABILIDAD DEL ÁREA REQUIRENTE Y TÉCNICA DEL ARRENDAMIENTO, ASÍ COMO LAS ACTAS CORRESPONDIENTES DE LAS JUNTAS DE ACLARACIONES CELEBRADAS.

TERCERA. IMPORTE DEL CONTRATO

LAS PARTES ACUERDAN QUE EL PRESENTE ES UN CONTRATO ABIERTO EN LOS TÉRMINOS DEL ARTÍCULO 47 DEL RAAS, POR LO QUE EL MONTO MÍNIMO TOTAL ASCIENDE A LA CANTIDAD DE **$10,931,027.96 (DIEZ MILLONES NOVECIENTOS TREINTA Y UNO MIL VEINTISIETE PESOS 96/100 M.N.)** MÁS LA CANTIDAD DE

$1,748,964.22 (UN MILLÓN SETECIENTOS CUARENTA Y OCHO MIL NOVECIENTOS SESENTA Y CUATRO PESOS 22/100 M.N.) POR EL CONCEPTO DEL I.V.A., DANDO UN TOTAL **DE $12,679,992.18 (DOCE MILLONES SEISCIENTOS SETENTA Y NUEVE MIL NOVECIENTOS NOVENTA Y DOS PESOS 18/100 M.N.)**.

EL MONTO MÁXIMO TOTAL ASCIENDE A LA CANTIDAD DE **$27,327,569.34 (VEINTISIETE MILLONES TRESCIENTOS VEINTISIETE MIL QUINIENTOS SESENTA Y NUEVE PESOS 34/100 M.N.)** MÁS LA CANTIDAD DE **$4,372,411.10 (CUATRO MILLONES TRESCIENTOS SETENTA Y DOS MIL CUATROCIENTOS ONCE PESOS 10/100 M.N.)** POR EL CONCEPTO DEL I.V.A., DANDO UN TOTAL DE **$31,699,980.44 (TREINTA Y UN MILLONES SEISCIENTOS NOVENTA Y NUEVE MIL NOVECIENTOS OCHENTA PESOS 44/100 M.N.)**, MISMOS QUE SERÁN ENTREGADOS DE LA SIGUIENTE FORMA.

	Del 01 de enero al 31 de diciembre de 2020	Del 01 de enero al 31 de diciembre de 2021	Del 01 de enero al 31 de diciembre de 2022	TOTAL
Máximo	$10,566,660.15	$10,566,660.15	$10,566,660.15	$31,699,980.44
Mínimo	$4,226,664.06	$4,226,664.06	$4,226,664.06	$12,679,992.18

EL IMPORTE DEL PRESENTE CONTRATO ES FIJO Y NO ESTARÁ SUJETO A FÓRMULA ESCALATORIA ALGUNA DURANTE LA VIGENCIA DEL PRESENTE CONTRATO, CON FUNDAMENTO EN EL ARTÍCULO 45, FRACCIÓN X DEL RAAS.

CUARTA. FORMA DE PAGO

EL **"INAI"** REALIZARÁ EL PAGO CORRESPONDIENTE AL **"PROVEEDOR"** DEL IMPORTE PACTADO EN LA CLÁUSULA QUE ANTECEDE POR EL SERVICIO OBJETO DE ESTE CONTRATO, CONFORME SE ESTABLECE EN EL ANEXO TÉCNICO, CONTRA ENTREGA Y ACEPTACIÓN DEL ARRENDAMIENTO EFECTIVAMENTE PRESTADO A ENTERA SATISFACCIÓN DE LA DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN, EN LOS TÉRMINOS PRECISADOS EN EL ANEXO TÉCNICO, MEDIANTE LA FACTURA CORRESPONDIENTE, A TRAVÉS DE DEPÓSITO O TRANSFERENCIA ELECTRÓNICA EN CUENTA BANCARIA DEL **"PROVEEDOR"**.

EL PLAZO MÁXIMO QUE DEBERÁ MEDIAR ENTRE LA FECHA EN QUE EL "**PROVEEDOR**" ACREDITE LA EJECUCIÓN DEL SERVICIO Y LA FECHA DE PAGO CORRESPONDIENTE SERÁ DENTRO DE 20 DÍAS NATURALES, EN TERMINOS DEL PRIMER PÁRRAFO DEL ARTÍCULO 50 DEL RAAS, CONTADOS A PARTIR DE LA FECHA EN QUE EL **"PROVEEDOR"** PRESENTE LA FACTURA CORRESPONDIENTE, LA CUAL DEBERÁ CUMPLIR CON LOS REQUISITOS FISCALES CONFORME A LA NORMATIVIDAD VIGENTE Y APLICABLE, EN EL SUPUESTO DE QUE LA FACTURA NO FUERA PRESENTADA, EL PAGO SE DIFERIRÁ POR EL MISMO PLAZO QUE SE TARDE EN SUBSANAR ESTA SITUACIÓN.

EL **"PROVEEDOR"** SE COMPROMETE A PRESTAR EL ARRENDAMIENTO OBJETO DEL PRESENTE CONTRATO CONFORME A LO SEÑALADO EN EL ANEXO TÉCNICO, LA DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN, SERÁ LA RESPONSABLE DE SU ACEPTACIÓN A ENTERA SATISFACCIÓN, SU DEVOLUCIÓN O RECHAZO, DETERMINAR LOS INCUMPLIMIENTOS AL PRESENTE INSTRUMENTO, ASI COMO DE HACER CUMPLIR LOS PLAZOS ESTABLECIDOS EN EL PÁRRAFO ANTERIOR.

EL INCUMPLIMIENTO EN LA EJECUCIÓN DEL SERVICIO DEBERÁ SER COMUNICADO AL **"PROVEEDOR"** A MÁS TARDAR AL DÍA HÁBIL SIGUIENTE A AQUÉL EN QUE ÉSTE SE DETERMINE, SEÑALANDO LAS RAZONES QUE LOS MOTIVARON, LAS CUALES DEBERÁN ESTAR VINCULADAS A LAS CONDICIONES ESTABLECIDAS EN ESTE CONTRATO, INDICANDO EL PLAZO PARA SU REANUDACIÓN O CORRECCIÓN. ESTA COMUNICACIÓN INTERRUMPE EL COMPUTO DEL PLAZO DE LA EJECUCIÓN DEL ARRENDAMIENTO Y EL MOMENTO EN QUE ESTE ES RECIBIDO A SATISFACCIÓN.

LA FACTURA DEBERÁ PRESENTARSE EN LA DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN DEL **"INAI"** UBICADA EN EL PRIMER PISO DE SUS INSTALACIONES EN UN HORARIO DE LUNES A VIERNES DE 9:00 A 15:00 HORAS Y DE LUNES A JUEVES DE 17:00 A 19:00 HORAS O BIEN, LOS ARCHIVOS ELECTRÓNICOS DE LA FACTURA (PDF Y XML) DEBERÁN SER ENVIADOS A LA DIRECCIÓN ELECTRÓNICA felipe.quintero@inai.org.mx.

DEBIENDO INMEDIATAMENTE TURNARLA A LA DIRECCIÓN DE RECURSOS FINANCIEROS A EFECTO DE VALIDAR QUE LA FACTURA CUMPLA CON LOS REQUISITOS FISCALES CORRESPONDIENTES Y AQUELLOS DE ACEPTACIÓN DEL SERVICIO QUE AMPAREN, EN CASO DE QUE LA FACTURA NO CUMPLA CON LOS REQUISITOS NECESARIOS, ÉSTA DIRECCIÓN DEVOLVERÁ A LA DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN QUIEN SERÁ LA RESPONSABLE DE DEVOLVER AL **"PROVEEDOR"** LA FACTURA DENTRO DE LOS TRES DÍAS HÁBILES SIGUIENTES AL DE SU RECEPCIÓN, COMUNICÁNDOLE LOS ERRORES O DEFICIENCIAS DETECTADAS.

EN EL CASO DE QUE SE COMUNIQUEN AL **"PROVEEDOR"** LA EXISTENCIA DE ERRORES O DEFICIENCIAS EN LA FACTURA, SERÁ RESPONSABLE DE SUBSANARLOS Y PRESENTAR NUEVAMENTE DICHA FACTURA QUE REÚNA LOS REQUISITOS FISCALES CORRESPONDIENTES EN EL MENOR TIEMPO POSIBLE.

POR LO ANTERIOR, EL TRÁMITE PARA EL PAGO DEL ARRENDAMIENTO SÓLO PODRÁ INICIARSE A PARTIR DE LA FECHA EN QUE LOS RESPONSABLES DE ADMINISTRAR EL PROYECTO POR PARTE DEL **"INAI"** HAYAN RECIBIDO A SU ENTERA SATISFACCIÓN EL MISMO DE CONFORMIDAD CON LAS ESPECIFICACIONES SEÑALADAS EN EL ANEXO TÉCNICO, Y SIEMPRE Y CUANDO EL **"PROVEEDOR"** HAYA ENTREGADO LA FACTURA CORRESPONDIENTE PARA SU TRÁMITE, Y LA MISMA CUMPLA CON LOS REQUISITOS FISCALES RESPECTIVOS EN TÉRMINOS DE LEY, EN CASO DE INCUMPLIMIENTO EN LOS PAGOS POR PARTE DEL **"INAI"** A SOLICITUD DEL **"PROVEEDOR"**, EL **"INAI"** DEBERÁ PAGAR GASTOS FINANCIEROS CONSIDERANDO ÚNICAMENTE LA TASA ESTABLECIDA POR LA LEY DE INGRESOS DE LA FEDERACIÓN, EN LOS CASOS DE PRÓRROGA PARA EL PAGO DE CRÉDITOS FISCALES, EN TÉRMINOS DE LO SEÑALADO POR EL ARTÍCULO 50 SEGUNDO PARRAFO DEL RAAS. DICHOS GASTOS SE CALCULARÁN SOBRE LAS CANTIDADES NO PAGADAS Y SE COMPUTARÁN POR DÍAS NATURALES DESDE QUE SE VENCIÓ EL PLAZO PACTADO, HASTA QUE SE PONGA EFECTIVAMENTE LAS CANTIDADES A DISPOSICIÓN DEL **"PROVEEDOR"**.

TRATÁNDOSE DE PAGOS EN EXCESO QUE HAYA RECIBIDO EL **"PROVEEDOR"** ESTE DEBERÁ DE REINTEGRAR LAS CANTIDADES PAGADAS EN EXCESO MÁS LOS INTERESES CORRESPONDIENTES CONFORME A LO SEÑALADO EN EL PÁRRAFO ANTERIOR. LOS INTERESES SE CALCULARÁN SOBRE LAS CANTIDADES PAGADAS EN EXCESO EN CADA CASO Y SE COMPUTARÁN POR DÍAS NATURALES DESDE LA FECHA DEL PAGO HASTA LA FECHA QUE SE PONGA EFECTIVAMENTE LAS CANTIDADES A DISPOSICIÓN DEL **"INAI"**.

A FIN DE ATENDER LAS DISPOSICIONES GENERALES A LAS QUE DEBERÁN SUJETARSE LAS DEPENDENCIAS Y ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA FEDERAL PARA SU INCORPORACIÓN AL PROGRAMA DE CADENAS PRODUCTIVAS DE NACIONAL FINANCIERA, S.N.C., PUBLICADAS EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 28 DE FEBRERO DE 2007, LA DIRECCIÓN DE RECURSOS FINANCIEROS, INCORPORARÁ AL PORTAL DE NACIONAL FINANCIERA, S.N.C., LOS PAGOS QUE SE GENEREN POR LA CONTRATACIÓN DE ESTE CONTRATO, A FIN DE QUE EL **"PROVEEDOR"** DECIDA SI EJERCERÁ LA CESIÓN DE LOS DERECHOS DE COBRO AL INTERMEDIARIO FINANCIERO POR ÉL SELECCIONADO DE ENTRE LOS REGISTRADOS EN DICHO PROGRAMA EN LOS TÉRMINOS DEL ÚLTIMO PÁRRAFO DEL ARTÍCULO 46 DEL RAAS.

QUINTA. VIGENCIA

EL **"PROVEEDOR"** SE OBLIGA A PRESTAR EL SERVICIO OBJETO DEL PRESENTE CONTRATO, A PARTIR DEL 01 DE ENERO DE 2020 Y HASTA EL 31 DE DICIEMBRE DE 2022.

SEXTA. GARANTÍA

PARA GARANTIZAR EL FIEL Y EXACTO CUMPLIMIENTO DE LAS OBLIGACIONES A SU CARGO EN TÉRMINOS DEL PRESENTE CONTRATO, EL **"PROVEEDOR"** QUEDA OBLIGADO A ENTREGAR CUALQUIERA DE LAS SIGUIENTES GARANTÍAS: CHEQUE CERTIFICADO O DE CAJA, BILLETE DE DEPÓSITO, O PÓLIZA DE FIANZA.

EN TÉRMINOS DEL CAPITULO X NUMERAL 2 FRACCIÓN VI DE LAS "BALINES" LA GARANTÍA DE CUMPLIMIENTO SE PODRÁ ENTREGAR POR MEDIOS ELECTRÓNICOS, SIEMPRE QUE LAS DISPOSICIONES JURÍDICAS APLICABLES PERMITAN LA CONSTITUCIÓN DE LAS GARANTÍAS POR DICHOS MEDIOS.

REVISADO - VO. BO. - DEPARTAMENTO LEGAL - PROMOTOR - GRUPOTECNO

EN CASO DE ENTREGAR FIANZA, EL **"PROVEEDOR"** SE OBLIGA A CONSTITUIR EN LA FORMA, TÉRMINOS Y PROCEDIMIENTOS PREVISTOS EN LOS ARTÍCULOS 48 DEL RAAS Y CAPITULO X NUMERAL 8 DE LAS "BALINES", DICHA GARANTÍA SE OTORGARÁ POR EL 10% (DIEZ POR CIENTO) DEL MONTO MÁXIMO TOTAL ANTES DE I.V.A. LA CUÁL SERÁ INDIVISIBLE, MISMA QUE ESTARÁ VIGENTE HASTA LA TOTAL ACEPTACIÓN DEL SERVICIO OBJETO DEL PRESENTE CONTRATO POR PARTE DEL **"INAI"**.

DICHA PÓLIZA DE FIANZA DEBERÁ PREVER, COMO MÍNIMO, LAS SIGUIENTES DECLARACIONES:

A) QUE LA FIANZA SE OTORGA ATENDIENDO A TODAS LAS ESTIPULACIONES CONTENIDAS EN EL CONTRATO;
B) QUE, PARA CANCELAR LA FIANZA, SERÁ REQUISITO CONTAR CON LA CONSTANCIA DE CUMPLIMIENTO TOTAL DE LAS OBLIGACIONES CONTRACTUALES;
C) QUE LA FIANZA PERMANECERÁ VIGENTE DURANTE EL CUMPLIMIENTO DE LA OBLIGACIÓN QUE GARANTICE Y CONTINUARÁ VIGENTE EN CASO DE QUE SE OTORGUE PRÓRROGA AL CUMPLIMIENTO DEL CONTRATO, ASÍ COMO DURANTE LA SUBSTANCIACIÓN DE TODOS LOS RECURSOS LEGALES O DE LOS JUICIOS QUE SE INTERPONGAN Y HASTA QUE SE DICTE RESOLUCIÓN DEFINITIVA QUE QUEDE FIRME, Y
D) QUE LA AFIANZADORA ACEPTA EXPRESAMENTE SOMETERSE A LOS PROCEDIMIENTOS DE EJECUCIÓN PREVISTOS EN LA LEY DE INSTITUCIONES DE SEGUROS Y FIANZAS PARA LA EFECTIVIDAD DE LAS FIANZAS, AÚN PARA EL CASO DE QUE PROCEDA EL COBRO DE INDEMNIZACIÓN POR MORA, CON MOTIVO DEL PAGO EXTEMPORÁNEO DEL IMPORTE DE LA PÓLIZA DE FIANZA REQUERIDA. TRATÁNDOSE DE DEPENDENCIAS, EL PROCEDIMIENTO DE EJECUCIÓN SERÁ EL PREVISTO EN EL ARTÍCULO 282 DE LA CITADA LEY, DEBIÉNDOSE ATENDER PARA EL COBRO DE INDEMNIZACIÓN POR MORA LO DISPUESTO EN EL ARTÍCULO 283 DE DICHA LEY.

LA GARANTÍA ANTES MENCIONADA DEBERÁ PRESENTARSE A MÁS TARDAR DENTRO DE LOS 10 DÍAS NATURALES SIGUIENTES A LA FIRMA DEL CONTRATO CON FUNDAMENTO EN LO ESTABLECIDO EN EL ARTÍCULO 48 DEL RAAS.

UNA VEZ CUMPLIDAS LAS OBLIGACIONES DEL **"PROVEEDOR"** A SATISFACCIÓN DEL **"INAI"**, EL DIRECTOR GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN PROCEDERA A EXTENDER LA CONSTANCIA DE CUMPLIMIENTO DE LAS OBLIGACIONES CONTRACTUALES PARA QUE SE DÉ INICIO A LOS TRÁMITES PARA LA CANCELACIÓN DE LA GARANTÍA PRESENTADA.

SÉPTIMA. SUPERVISIÓN

LAS PARTES MANTENDRÁN LOS REGISTROS NECESARIOS DE LAS ACTIVIDADES REALIZADAS CON MOTIVO DE LA EJECUCIÓN DEL ARRENDAMIENTO OBJETO DEL PRESENTE CONTRATO.

"INAI"	"PROVEEDOR"
NOMBRE: JOSÉ ÁNGEL ESPARZA PORTUGAL	NOMBRE: JORGE RAMOS
DIRECCIÓN: AVENIDA INSURGENTES SUR 3211, COLONIA INSURGENTES CUICUILCO, ALCALDÍA COYOACÁN, C.P. 04530, CIUDAD DE MÉXICO	DIRECCIÓN: CALLE REVOLUCIÓN 1145, COLONIA MERCED GÓMEZ, ALCALDÍA BENITO JUÁREZ, CÓDIGO POSTAL 03930, CIUDAD DE MÉXICO.
TELÉFONO:5004 2400 EXT. 2436	TELÉFONO: 5550598703
CORREO ELECTRÓNICO: angel.esparza@inai.org.mx	CORREO ELECTRÓNICO: jorge.ramos@tecno.com.mx

EL **"INAI"**, A TRAVÉS DEL REPRESENTANTE DESIGNADO EN ÉSTA CLAUSULA, TENDRÁ EN TODO TIEMPO EL DERECHO DE SUPERVISAR LA EJECUCIÓN DEL SERVICIO POR ARRENDAMIENTO SIN OPCIÓN DE COMPRA

CONTRATADO Y DARÁ POR ESCRITO AL **"PROVEEDOR"** LAS INSTRUCCIONES QUE ESTIME PERTINENTES CON RELACIÓN A SU EJECUCIÓN, SIN QUE ELLO IMPLIQUE VARIAR LAS CONDICIONES QUE SE PRECISAN EN EL ANEXO TÉCNICO DEL PRESENTE INSTRUMENTO.

EL **"PROVEEDOR"** SE COMPROMETE A PRESTAR EL ARRENDAMIENTO OBJETO DE ESTE CONTRATO EN LOS LUGARES Y CONFORME A LOS TÉRMINOS Y CONDICIONES ESTIPULADOS EN EL ANEXO TÉCNICO DEL MISMO.

POR SU PARTE, EL DIRECTOR GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN DEL **"INAI"** SERA EL SERVIDOR PÚBLICO FACULTADO PARA RECIBIR EL ARRENDAMIENTO PRESTADO, ASIMISMO, SERÁ TAMBIÉN RESPONSABLE DE LA ACEPTACIÓN DEL ARRENDAMIENTO A SU ENTERA SATISFACCIÓN, VERIFICANDO EN TODO MOMENTO QUE SE REALICEN DE CONFORMIDAD CON LO ESTIPULADO EN EL ANEXO TÉCNICO, POR LO QUE EL **"PROVEEDOR"** MANIFIESTA SU CONFORMIDAD DE QUE EN TANTO ELLO NO SE CUMPLA, NO SE TENDRÁN POR RECIBIDO O ACEPTADO.

EL DIRECTOR GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN DEL **"INAI"** SERA EL SERVIDOR PÚBLICO FACULTADO DE DETERMINAR EN SU CASO, LOS INCUMPLIMIENTOS A LOS TÉRMINOS PACTADOS, ASÍ COMO DE HACER CUMPLIR LOS PLAZOS QUE HUBIEREN ESTABLECIDO LAS PARTES PARA LA EJECUCIÓN DE LOS MISMOS.

DETERMINADO EL INCUMPLIMIENTO EN LA PRESTACIÓN DEL ARRENDAMIENTO, EL MISMO DEBERÁ SER COMUNICADO AL **"PROVEEDOR"** A MÁS TARDAR EL DÍA HÁBIL SIGUIENTE A AQUEL EN QUE ÉSTE SE DETERMINE, SEÑALANDO LAS RAZONES QUE LO MOTIVARON, LAS CUALES DEBERÁN ESTAR VINCULADAS A LAS CONDICIONES ESTABLECIDAS EN EL ANEXO TÉCNICO, INDICANDO EL PLAZO PARA SU REPOSICIÓN O CORRECCIÓN.

EL COMPUTO DEL PLAZO ENTRE EL MOMENTO EN EL QUE SE CONCLUYE ARRENDAMIENTO SIN OPCIÓN A COMPRA Y EL MOMENTO EN QUE ÉSTE ES RECIBIDO A SATISFACCIÓN, SE INTERRUMPIRÁ CUANDO EL **"INAI"** ACREDITE HABER COMUNICADO AL **"PROVEEDOR"** EL INCUMPLIMIENTO EN LOS TÉRMINOS ESTABLECIDOS EN EL PÁRRAFO ANTERIOR.

LOS DÍAS QUE TRANSCURRAN ENTRE LA FECHA EN QUE EL **"INAI"** NOTIFIQUE AL **"PROVEEDOR"** EL INCUMPLIMIENTO EN EL ARRENDAMIENTO SIN OPCIÓN DE COMPRA Y AQUELLA EN LA QUE ÉSTE REALICE LA CORRECCIÓN RESPECTIVA DIFERIRÁN EN IGUAL PLAZO LA FECHA PARA LA RECEPCIÓN DE LOS MISMOS A SATISFACCIÓN.

OCTAVA. RESPONSABILIDADES DEL "PROVEEDOR"

EL **"PROVEEDOR"** SERÁ EL ÚNICO RESPONSABLE DE QUE EL ARRENDAMIENTO SE REALICE DE CONFORMIDAD CON LO ESTIPULADO EN EL PRESENTE INSTRUMENTO, EN EL ANEXO TÉCNICO Y EN LAS INSTRUCCIONES QUE POR ESCRITO LE NOTIFIQUE EL **"INAI"**, Y QUE NO IMPLIQUEN UNA VARIACIÓN EN LAS CONDICIONES ESPECIFICADAS EN EL ANEXO TÉCNICO, EN CASO CONTRARIO EL **"PROVEEDOR"** DEBERÁ REALIZAR LAS MODIFICACIONES NECESARIAS, MISMAS QUE SERÁN POR SU CUENTA Y RIESGO, SIN QUE TENGA DERECHO A RETRIBUCIÓN ALGUNA POR CONCEPTO DE DICHAS MODIFICACIONES. SI EL **"PROVEEDOR"** NO ATENDIERE LOS REQUERIMIENTOS DEL **"INAI"**, ESTE ÚLTIMO PODRÁ ENCOMENDAR A UN TERCERO LA MODIFICACIÓN DE QUE SE TRATE, CON CARGO AL **"PROVEEDOR"**. LO ANTERIOR SIN PERJUICIO DE LA APLICACIÓN DE LAS PENAS CONVENCIONALES POR ATRASO QUE, EN SU CASO, RESULTEN PROCEDENTES.

ASIMISMO, EL **"PROVEEDOR"** RESPONDERÁ ANTE EL **"INAI"** POR SU CUENTA Y RIESGO DE CUALQUIER DEFECTO O VICIO OCULTO EN LA EJECUCIÓN DEL SERVICIO, ASÍ COMO DE CUALQUIER OTRA RESPONSABILIDAD EN QUE HUBIERE INCURRIDO, EN LOS TÉRMINOS DE LA LEGISLACIÓN APLICABLE.

DEPARTAMENTO LEGAL - REVISADO - YO ME DOMICILIO

NOVENA. DAÑOS Y PERJUICIOS

EL **"PROVEEDOR"** SE OBLIGA A RESPONDER POR SU CUENTA Y RIESGO DE LOS DAÑOS Y PERJUICIOS QUE POR INOBSERVANCIA O NEGLIGENCIA DE SU PARTE SE LLEGUEN A CAUSAR A EL **"INAI"** O A TERCEROS, EN CUYO CASO SE OBLIGA A RESARCIR LOS DAÑOS Y PERJUICIOS CAUSADOS, INDEPENDIENTEMENTE DE LA MULTA Y/O INHABILITACIÓN QUE SE LE IMPONGAN EN TÉRMINOS DE LOS ARTÍCULOS 62 Y 63 DEL RAAS.

DÉCIMA. CESIÓN DE DERECHOS Y OBLIGACIONES

EL **"PROVEEDOR"** SE OBLIGA A NO CEDER EN FORMA PARCIAL NI TOTAL, A NINGUNA PERSONA, LOS DERECHOS Y OBLIGACIONES DERIVADAS DEL PRESENTE CONTRATO, A EXCEPCIÓN DE LOS DERECHOS DE COBRO, EN CUYO CASO SE DEBERÁ DE CONTAR CON EL CONSENTIMIENTO PREVIO Y POR ESCRITO DEL **"INAI"**.

DÉCIMA PRIMERA. IMPUESTOS

LOS IMPUESTOS QUE SE GENEREN POR ARRENDAMIENTO SIN OPCIÓN A COMPRA OBJETO DEL PRESENTE CONTRATO, SE PAGARÁN Y ENTERARÁN POR QUIEN LOS CAUSE, CONFORME A LA LEGISLACIÓN FISCAL VIGENTE.

DÉCIMA SEGUNDA. PROPIEDAD DE LA INFORMACIÓN

LA INFORMACIÓN FUENTE PROPORCIONADA POR EL **"INAI"**, ASÍ COMO LA QUE RESULTE DEL ARRENDAMIENTO SIN OPCIÓN A COMPRA OBJETO DE ESTE CONTRATO, SERÁ EN TODO MOMENTO PROPIEDAD EXCLUSIVA DEL **"INAI"**, Y SERÁ PÚBLICA EN LOS TÉRMINOS Y CON LAS RESTRICCIONES QUE ESTABLECEN LA LFTAIP Y NORMATIVIDAD APLICABLE.

DÉCIMA TERCERA. LUGAR DEL ARRENDAMIENTO SIN OPCIÓN A COMPRA

EL ARRENDAMIENTO OBJETO DEL PRESENTE CONTRATO SERÁ PROVISTO EN EL **"INAI"** UBICADA EN AV. INSURGENTES SUR 3211, COL. INSURGENTES CUICUILCO, ALCALDÍA COYOACÁN, C.P. 04530 EN LA CIUDAD DE MÉXICO, DE ACUERDO A LAS CARACTERÍSTICAS Y ESPECIFICACIONES DESCRITAS EN EL ANEXO TÉCNICO.

DÉCIMA CUARTA. AMPLIACIÓN DEL CONTRATO

EL **"INAI"** PODRÁ, DENTRO DE SU PRESUPUESTO APROBADO Y DISPONIBLE, BAJO SU RESPONSABILIDAD Y POR RAZONES FUNDADAS Y EXPLÍCITAS, ACORDAR EL INCREMENTO DEL MONTO DEL PRESENTE CONTRATO, O DE LA CANTIDAD DEL ARRENDAMIENTO SOLICITADO MEDIANTE MODIFICACIONES AL MISMO DURANTE SU PERIODO DE VIGENCIA, SIEMPRE QUE LAS MODIFICACIONES NO REBASEN, EN CONJUNTO, EL 20% (VEINTE POR CIENTO) DEL MONTO MÁXIMO TOTAL O CANTIDAD DE LOS CONCEPTOS O VOLÚMENES ESTABLECIDOS EN EL CONTRATO Y EL PRECIO DEL ARRENDAMIENTO SEA IGUAL AL PACTADO ORIGINALMENTE.

DE CONFORMIDAD CON EL ARTÍCULO 51 DEL RAAS, EL PORCENTAJE AL QUE SE HACE REFERENCIA EN EL PÁRRAFO ANTERIOR, SE APLICARÁ PARA CADA PARTIDA O CONCEPTO, ENTENDIÉNDOSE ÉSTOS COMO LA DIVISIÓN O DESGLOSE DEL ARRENDAMIENTO A CONTRATAR, CONTENIDOS EN UN PROCEDIMIENTO DE CONTRATACIÓN O EN UN CONTRATO, PARA DIFERENCIARLOS UNOS DE OTROS, CLASIFICARLOS O AGRUPARLOS.

DE ACUERDO A LO DISPUESTO EN EL CAPITULO XI NUMERAL 2 DE LAS "BALINES", ÚNICAMENTE SE PODRÁ AMPLIAR EL PLAZO ORIGINALMENTE PACTADO PARA EL ARRENDAMIENTO SIN OPCIÓN A COMPRA, O BIEN LA VIGENCIA DEL CONTRATO, CUANDO ELLO SEA NECESARIO EN VIRTUD DEL ATRASO DEL **"PROVEEDOR"** EN LA PRESTACIÓN DE AQUELLOS, SIEMPRE QUE EL ATRASO HAYA SIDO ORIGINADO POR CASO FORTUITO, FUERZA MAYOR O POR CAUSAS ATRIBUIBLES AL **"INAI"**, SIEMPRE Y CUANDO DICHA MODIFICACIÓN NO IMPLIQUE INCREMENTO EN EL MONTO MÁXIMO TOTAL DEL CONTRATO LA MODIFICACIÓN SE FORMALIZARÁ MEDIANTE

LA SUSCRIPCIÓN DE UN CONVENIO Y EL **"INAI"** INTEGRARÁ AL EXPEDIENTE RESPECTIVO LA CONSTANCIA QUE ACREDITE LA ACTUALIZACIÓN DE DICHOS SUPUESTOS.

LAS MODIFICACIONES EN MONTO PLAZO O VIGENCIA AL CONTRATO, CONLLEVARÁ EL RESPECTIVO AJUSTE A LA GARANTÍA DE CUMPLIMIENTO, PARA LO CUAL DEBERÁ ESTIPULARSE EN EL CONVENIO MODIFICATORIO RESPECTIVO EL PLAZO PARA ENTREGAR LA AMPLIACIÓN DE GARANTÍA, EL CUAL NO DEBERÁ EXCEDER DE 10 (DIEZ) DÍAS NATURALES SIGUIENTES A LA FIRMA DEL CONVENIO, ASÍ COMO ESTABLECERSE LA FECHA PARA LA PRESTACIÓN DEL ARRENDAMIENTO PARA LAS CANTIDADES ADICIONALES, TRATÁNDOSE DE FIANZA, EL AJUSTE CORRESPONDIENTE SE REALIZARÁ CONFORME A LO DISPUESTO POR LA FRACCIÓN II Y IV DEL PENÚLTIMO PÁRRAFO DEL NUMERAL 8 CAPITULO X DE LAS "BALINES".

DÉCIMA QUINTA. PENAS CONVENCIONALES

LAS PENAS CONVENCIONALES SE DETERMINARÁN EN FUNCIÓN DEL ARRENDAMIENTO NO PRESTADO OPORTUNAMENTE, A RAZÓN DEL 1% (UNO POR CIENTO) DIARIO SOBRE EL PRECIO MENSUAL DE LOS MISMOS ANTES DEL I.V.A., POR CADA DÍA NATURAL DE ATRASO Y ESTA SE HARÁ EFECTIVA CON CARGO AL IMPORTE DEL ARRENDAMIENTO PENDIENTE DE PAGO. EN NINGÚN MOMENTO LAS PENAS CONVENCIONALES EXCEDERÁN EL 10% DEL MONTO MÁXIMO TOTAL DEL PRESENTE INSTRUMENTO, ANTES DEL I.V.A. DE CONFORMIDAD CON EL CAPÍTULO XI, NUMERAL 3 DE LAS "BALINES".

EN CASO DE QUE PROCEDIERA LA APLICACIÓN DE PENAS CONVENCIONALES, EL **"PROVEEDOR"**, PAGARÁ EL IMPORTE DE LAS MISMAS, MEDIANTE NOTA DE CRÉDITO O DE DEPÓSITO EN CUENTA BANCARIA DEL **"INAI"** 0252038954 DEL BANCO BANORTE.

EL DIRECTOR GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN, RESPONSABLE DEL ARRENDAMIENTO CONTRATADO, FORMULARÁ LOS INFORMES SOBRE LOS ATRASOS EN EL CUMPLIMIENTO DE LAS OBLIGACIONES DEL **"PROVEEDOR"** Y LLEVARÁ A CABO EL TRÁMITE CORRESPONDIENTE.

EL PAGO DEL ARRENDAMIENTO PRESTADO EN TIEMPO QUEDARÁ CONDICIONADO AL PAGO QUE DEBA HACER EL **"PROVEEDOR"**, DE LAS PENAS CONVENCIONALES QUE EN SU CASO LE SEAN IMPUESTAS.

DÉCIMA SEXTA. DEDUCCIONES

DE CONFORMIDAD CON LO ESTABLECIDO EN EL ARTÍCULO 53, DEL RAAS DEL **"INAI"**, ASÍ COMO EL CAPÍTULO XI, NUMERAL 4 DE LAS BALINES, SE APLICARÁ AL **"PROVEEDOR"** LAS DEDUCTIVAS QUE SE ENLISTAN A CONTINUACIÓN, POR EL ARRENDAMIENTO PRESTADO DE MANERA PARCIAL O DEFICIENTE REFERENTE A LA FACTURACIÓN MENSUAL QUE CORRESPONDA, POR DICHOS SERVICIOS, TENIENDO EN CUENTA QUE LA DEDUCTIVA NO PODRÁ EXCEDER DE 8% DEL MONTO MÁXIMO TOTAL DEL PRESENTE INSTRUMENTO, ANTES DEL I.V.A.

CUANDO EL ATRASO DEL **"PROVEEDOR"** EN LA PRESTACIÓN DEL ARRENDAMIENTO SE DEBA A CASO FORTUITO, FUERZA MAYOR O CAUSAS ATRIBUIBLES AL **"INAI"**, NO PROCEDERÁ LA APLICACIÓN DE DICHAS DEDUCCIONES.

DÉCIMA SÉPTIMA. TERMINACIÓN ANTICIPADA

AMBAS PARTES ACUERDAN EN QUE EL **"INAI"** PODRÁ DAR POR TERMINADO EL PRESENTE CONTRATO EN CUALQUIER MOMENTO SIN RESPONSABILIDAD PARA EL **"INAI"**, DANDO AVISO POR ESCRITO AL **"PROVEEDOR"**, POR CONDUCTO DE SU REPRESENTANTE LEGAL Y/O EL RESPONSABLE SEÑALADO EN LA CLÁUSULA SÉPTIMA DEL PRESENTE INSTRUMENTO, CUANDO CONCURRAN RAZONES DE INTERÉS GENERAL O BIEN, CUANDO POR CAUSAS JUSTIFICADAS SE EXTINGA LA NECESIDAD DE REQUERIR EL ARRENDAMIENTO ORIGINALMENTE CONTRATADO, Y SE DEMUESTRE QUE DE CONTINUAR CON EL CUMPLIMIENTO DE LAS

OBLIGACIONES PACTADAS, SE OCASIONARÍA ALGÚN DAÑO O PERJUICIO AL ESTADO, O SE DETERMINE LA NULIDAD DE LOS ACTOS QUE DIERON ORIGEN AL CONTRATO, CON MOTIVO DE LA RESOLUCIÓN DE UNA INCONFORMIDAD O INTERVENCIÓN DE OFICIO EMITIDA POR EL ÓRGANO INTERNO DE CONTROL DEL INAI LO ANTERIOR CON FUNDAMENTO EN EL ARTÍCULO 55 DEL RAAS.

EN TÉRMINOS DEL CAPITULO XI, NUMERAL 5 DE LAS "BALINES" LA TERMINACIÓN ANTICIPADA DE LOS CONTRATOS Y LA SUSPENSIÓN DEL ARRENDAMIENTO SIN OPCIÓN A COMPRA SE SUSTENTARÁN MEDIANTE DICTAMEN QUE PRECISE LAS RAZONES O LAS CAUSAS JUSTIFICADAS QUE DEN ORIGEN A LAS MISMAS.

EN CASO DE QUE EL **"INAI"** DECIDA TERMINAR ANTICIPADAMENTE EL PRESENTE CONTRATO, PARA EL PAGO DE LOS GASTOS NO RECUPERABLES SE REQUERIRÁ LA SOLICITUD PREVIA Y POR ESCRITO DEL **"PROVEEDOR"** Y DICHO PAGO SERÁ PROCEDENTE CUANDO LOS MENCIONADOS GASTOS SEAN RAZONABLES, ESTÉN DEBIDAMENTE COMPROBADOS Y SE RELACIONEN DIRECTAMENTE CON EL CONTRATO.

EL **"PROVEEDOR"** PODRÁ SOLICITAR AL **"INAI"** EL PAGO DE GASTOS NO RECUPERABLES EN UN PLAZO MÁXIMO DE UN MES, CONTADO A PARTIR DE LA FECHA DE LA TERMINACIÓN ANTICIPADA DEL CONTRATO O DE LA SUSPENSIÓN DEL SERVICIO, SEGÚN CORRESPONDA.

LOS GASTOS NO RECUPERABLES POR ESTOS SUPUESTOS, SERÁN PAGADOS DENTRO DE UN TÉRMINO QUE NO PODRÁ EXCEDER DE CUARENTA Y CINCO DÍAS NATURALES POSTERIORES A LA SOLICITUD FUNDADA Y DOCUMENTADA DEL "**PROVEEDOR**". EN TÉRMINOS DEL CAPITULO XI, NUMERAL 8 DE LAS "BALINES".

DÉCIMA OCTAVA. RESCISIÓN

EL **"INAI"** PODRÁ RESCINDIR ADMINISTRATIVAMENTE EL PRESENTE CONTRATO POR CUALQUIERA DE LAS CAUSAS QUE A CONTINUACIÓN SE ENUMERAN:

1. SI EL **"PROVEEDOR"** SUSPENDE INJUSTIFICADAMENTE EL ARRENDAMIENTO SIN OPCIÓN A COMPRA AL QUE SE OBLIGÓ EN EL PRESENTE CONTRATO.
2. SI EL **"PROVEEDOR"** NO EJECUTA EL ARRENDAMIENTO DE CONFORMIDAD CON LO ESTIPULADO EN EL ANEXO TÉCNICO DE ESTE CONTRATO O SIN MOTIVO JUSTIFICADO NO ACATA LAS INSTRUCCIONES DEL **"INAI"**.
3. SI EL **"PROVEEDOR"** NO DA AL **"INAI"**, Y A LAS INSTANCIAS QUE TENGAN QUE INTERVENIR, LAS FACILIDADES Y DATOS NECESARIOS PARA LA INSPECCIÓN DEL ARRENDAMIENTO OBJETO DEL PRESENTE CONTRATO.
4. SI EL **"PROVEEDOR"** SE DECLARA EN CONCURSO MERCANTIL O SI HACE CESIÓN DEL ARRENDAMIENTO EN FORMA QUE AFECTE EL PRESENTE CONTRATO.
5. PORQUE EL **"PROVEEDOR"** TRANSMITA, TOTAL O PARCIALMENTE, LOS DERECHOS Y OBLIGACIONES DERIVADOS DE ESTE CONTRATO, CON EXCEPCIÓN DE LO SEÑALADO EN LA CLÁUSULA DÉCIMA DE ESTE INSTRUMENTO.
6. EN GENERAL POR INCUMPLIMIENTO O VIOLACIÓN DEL **"PROVEEDOR"** A CUALQUIERA DE LAS OBLIGACIONES DERIVADAS DEL PRESENTE CONTRATO.

EN CASO DE INCUMPLIMIENTO POR PARTE DEL **"PROVEEDOR"** DE CUALQUIERA DE LAS OBLIGACIONES CONSIGNADAS A SU CARGO EN ESTE INSTRUMENTO, EL **"INAI"** PODRÁ DETERMINAR LA RESCISIÓN DEL PRESENTE CONTRATO.

DÉCIMA NOVENA. PROCEDIMIENTO DE RESCISIÓN

SI EL **"INAI"** CONSIDERA QUE EL **"PROVEEDOR"** HA INCURRIDO EN ALGUNA DE LAS CAUSAS DE RESCISIÓN CONSIGNADAS EN LA CLÁUSULA QUE ANTECEDE, LO COMUNICARÁ POR ESCRITO A ESTE ÚLTIMO, POR CONDUCTO DE SU REPRESENTANTE LEGAL Y/O EL RESPONSABLE SEÑALADO EN LA CLÁUSULA SÉPTIMA ANTERIOR, PARA QUE EN UN MÁXIMO DE 5 DÍAS HÁBILES EXPONGA LO QUE A SU DERECHO CONVENGA RESPECTO DEL INCUMPLIMIENTO DE SU OBLIGACIÓN Y OFREZCA LAS PRUEBAS QUE ESTIME CONVENIENTES.

SI TRANSCURRIDO ESTE PLAZO EL **"PROVEEDOR"** NO HACE MANIFESTACIÓN ALGUNA EN SU DEFENSA, O SI DESPUÉS DE ANALIZAR LAS RAZONES ADUCIDAS POR ESTE, EL **"INAI"** ESTIMA QUE LAS MISMAS NO SON SATISFACTORIAS, PODRÁ DESDE LUEGO RESCINDIR ADMINISTRATIVAMENTE EL CONTRATO, DE ACUERDO CON LO DISPUESTO EN EL ARTÍCULO 54 DEL RAAS Y FORMULARÁ EL FINIQUITO CORRESPONDIENTE A EFECTO DE HACER CONSTAR LOS PAGOS QUE SE DEBAN EFECTUAR POR EL ARRENDAMIENTO PRESTADO HASTA EL MOMENTO DE LA RESCISIÓN.

EN CASO DE RESCINDIR EL PRESENTE CONTRATO, NO PROCEDERÁ EL COBRO DE PENAS CONVENCIONALES O SU CONTABILIZACIÓN, TODA VEZ QUE SE HARA EFECTIVA LA GARANTIA DE CUMPLIMIENTO ESTABLECIDA EN LA CLAUSULA SEXTA.

SI EL **"PROVEEDOR"** DECIDE RESCINDIR LA PRESENTE CONTRATACIÓN, SERÁ NECESARIO QUE ACUDA ANTE LA AUTORIDAD JUDICIAL FEDERAL COMPETENTE, A FIN DE OBTENER LA DECLARACIÓN CORRESPONDIENTE, EN TÉRMINOS DE LO SEÑALADO POR EL CAPÍTULO XI, NUMERAL 5 SEGUNDO PÁRRAFO DE LOS LINEAMIENTOS DE LAS "BALINES".

VIGÉSIMA. CASO FORTUITO O FUERZA MAYOR

NINGUNA DE LAS PARTES EN ESTE CONTRATO SERÁ RESPONSABLE POR EL RETRASO EN EL CUMPLIMIENTO DE SUS OBLIGACIONES DEBIDO A CASO FORTUITO O FUERZA MAYOR.

SE ENTIENDE POR CASO FORTUITO EL ACONTECIMIENTO NATURAL INEVITABLE, PREVISIBLE O IMPREVISIBLE, QUE IMPIDE EN FORMA ABSOLUTA EL CUMPLIMIENTO DE LA OBLIGACIÓN (TERREMOTOS, INUNDACIONES, ETC. SIENDO ESTAS ENUNCIATIVAS MÁS NO LIMITATIVAS).

SE ENTIENDE POR FUERZA MAYOR, EL HECHO DEL HOMBRE PREVISIBLE O IMPREVISIBLE, PERO INEVITABLE QUE IMPIDE EN FORMA ABSOLUTA EL CUMPLIMIENTO DE UNA OBLIGACIÓN (HUELGAS, GUERRAS, RESTRICCIONES GUBERNAMENTALES, ETC. SIENDO ESTAS ENUNCIATIVAS MÁS NO LIMITATIVAS).

EN TÉRMINOS DE LO SEÑALADO POR EL CAPITULO XI NUMERAL 2 DE LAS "BALINES", ANTE EL CASO FORTUITO O FUERZA MAYOR, O POR CAUSAS ATRIBUIBLES AL **"INAI"**, SE PODRÁN MODIFICAR LOS CONTRATOS A EFECTO DE PRORROGAR LA FECHA O PLAZO PARA LA ENTREGA DEL ARRENDAMIENTO. EN ESTE SUPUESTO DEBERÁ FORMALIZARSE EL CONVENIO MODIFICATORIO RESPECTIVO, NO PROCEDIENDO LA APLICACIÓN DE PENAS CONVENCIONALES POR ATRASO. TRATÁNDOSE DE CAUSAS IMPUTABLES AL **"INAI"**, NO SE REQUERIRÁ DE LA SOLICITUD DEL **"PROVEEDOR"**.

VIGÉSIMA PRIMERA. RELACIONES LABORALES

EL **"PROVEEDOR"**, COMO PATRÓN DEL PERSONAL QUE OCUPE PARA CUMPLIR EL OBJETO DE ESTE CONTRATO, SERÁ EL ÚNICO RESPONSABLE DE LAS OBLIGACIONES DERIVADAS DE TODOS LOS ORDENAMIENTOS EN MATERIA, CIVIL, PENAL, ADMINISTRATIVA, LABORAL Y DE SEGURIDAD SOCIAL, SIENDO ÉSTAS ENUNCIATIVAS MAS NO LIMITATIVAS.

EL **"PROVEEDOR"** CONVIENE POR LO MISMO EN RESPONDER DE TODAS LAS RECLAMACIONES QUE SUS TRABAJADORES PRESENTEN EN SU CONTRA O EN CONTRA DE EL **"INAI"** EN RELACIÓN CON ESTE CONTRATO, OBLIGÁNDOSE A SACAR A SALVO Y EN PAZ AL ORGANISMO.

VIGÉSIMA SEGUNDA. LEY APLICABLE

PARA LA INTERPRETACIÓN Y CUMPLIMIENTO DEL PRESENTE CONTRATO, LAS PARTES SE OBLIGAN A SUJETARSE ESTRICTAMENTE A TODAS Y CADA UNA DE LAS CLÁUSULAS Y ANEXOS QUE LO INTEGRAN, ASÍ COMO AL RAAS, BALINES Y TODA LA NORMATIVIDAD VIGENTE QUE RESULTE APLICABLE.

REVISADO - VO.BO. - DEPARTAMENTO LEGAL - GRUPOTECNO

EN CASO DE DISCREPANCIA ENTRE EL PRESENTE CONTRATO; Y LO CONTENIDO EN LA CONVOCATORIA Y SUS JUNTAS DE ACLARACIONES, PREVALECERÁ LO ESTIPULADO EN ÉSTAS, EN TÉRMINOS DE LO DISPUESTO EN EL CAPÍTULO X, NUMERAL 2, FRACCIÓN IV DE LAS BALINES.

VIGÉSIMA TERCERA. JURISDICCIÓN

PARA LA INTERPRETACIÓN, Y CUMPLIMIENTO DEL PRESENTE CONTRATO, LAS PARTES SE SOMETEN A LA JURISDICCIÓN Y COMPETENCIA DE LOS TRIBUNALES FEDERALES EN LA CIUDAD DE MÉXICO, RENUNCIANDO A LA QUE PUDIERE CORRESPONDERLES EN RAZÓN DE SU DOMICILIO PRESENTE O FUTURO O POR CUALQUIER OTRA CAUSA.

VIGÉSIMA CUARTA. INFORMACIÓN Y VERIFICACIÓN

EL **"PROVEEDOR"** SE COMPROMETE A PROPORCIONAR EN TODO MOMENTO, DE CONFORMIDAD CON EL CAPÍTULO XII, SEXTO PÁRRAFO DE LAS "BALINES", TODA LA INFORMACIÓN Y/O DOCUMENTACIÓN RELACIONADA CON EL PRESENTE CONTRATO, AL ÓRGANO INTERNO DE CONTROL DEL **"INAI"**, CON MOTIVO DE LAS AUDITORIAS, VISITAS O INSPECCIONES QUE PRACTIQUEN EN EJERCICIO DE SUS FACULTADES LEGALES.

LEÍDO EL PRESENTE INSTRUMENTO Y ENTERADAS LAS PARTES DE SU CONTENIDO Y ALCANCE DE TODAS LAS CLÁUSULAS, LO FIRMAN EN CINCO TANTOS ORIGINALES EN LA CIUDAD DE MÉXICO, A LOS DIECINUEVE DÍAS DEL MES DE DICIEMBRE DEL AÑO 2019----------

POR EL "INAI"	POR EL "PROVEEDOR"
LIC. RAFAEL ESTRADA CABRAL **APODERADO LEGAL**	**SELENE ELIZABETH CASTAÑON GUTIERREZ** **REPRESENTANTE LEGAL**
ING. JOSÉ LUIS HERNÁNDEZ SANTANA **DIRECTOR GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN**	

ÚLTIMA HOJA DEL CONTRATO DE PRESTACIÓN DE ARRENDAMIENTO SIN OPCIÓN A COMPRA, QUE CELEBRAN EL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES Y GRUPO DE TECNOLOGÍA CIBERNÉTICA, S.A. DE C.V. CELEBRADO EN LA CIUDAD DE MÉXICO, EL 6 DE DICIEMBRE DE 2019. ----------

DEPARTAMENTO LEGAL - REVISADO - YO ME COMPROMETO - GRUPOTECNO

1. INTRODUCCIÓN

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (**INAI**) a través de la Dirección General de Tecnologías de la Información (DGTI) requiere arrendar una solución (software y hardware) que le permita contar con la infraestructura tecnológica requerida, así como los servicios profesionales y el soporte técnico especializado, para mantener la seguridad y disponibilidad del tráfico que cursa por los enlaces a Internet, tanto de entrada como de salida. Así mismo requiere que se mantenga y mejore el nivel de seguridad externo (perimetral) e interno, a través de una solución de nueva generación para el control de accesos, protección de intrusos y ataques de nueva generación. Permitiendo así el acceso interno y remoto de sus usuarios en forma segura y controlada a los recursos del Instituto.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Contar con un contrato de arrendamiento sin opción a compra por un periodo de treinta y seis meses para proveer al INAI a través de la DGTI, una solución integral (software, hardware y servicios profesionales de implementación y soporte técnico especializado) en alta disponibilidad con un despliegue arquitectónico de seguridad en capas que permita mantener disponible y seguro el tráfico que cursa por los enlaces a Internet, tanto de entrada como de salida y al mismo tiempo que mejore el nivel de seguridad perimetral e interno actual a través de una solución de dispositivos de nueva generación para el control de accesos, protección de intrusos y ataques de nueva generación.

Nota: Al referirse a Hardware en este documento deberá entenderse como **"Hardware de uso específico"** para la aplicación de seguridad ofertada, el cual deberá ser provisto y garantizado como producto comercial vigente y nuevo por el fabricante de la solución ofertada, además de proveer el soporte al mismo durante la vigencia del contrato.

2.2. OBJETIVOS ESPECÍFICOS:

- Disponer de una solución para el balanceo de carga con alta disponibilidad de los enlaces a Internet con que cuenta el Instituto con una capacidad mínima de 200 Mbps por cada punta para asegurar futuros crecimientos.
- Disponer de una solución de seguridad perimetral de última generación para el control de acceso (*NGFW New Generation Firewall*), prevención y detección de intrusos (IDPS *Intrusion Detection and Prevention Systems*), balanceo de enlaces, protección de aplicaciones *web, protección avanzada para servidores y* detección y protección contra amenazas avanzadas
- La solución de seguridad perimetral deberá permitir el acceso controlado y seguro de usuarios remotos del Instituto a recursos internos, desde diferentes dispositivos / plataformas clientes y desde diferentes ubicaciones físicas a través de VPN´s (Virtual Private Network).
- Contar con los servicios profesionales de implementación, soporte y mantenimiento necesarios para asegurar la correcta operación de todos los componentes de la solución. Servicios que deben contar con experiencia probada en:
    - Implementación de la solución integral de seguridad redes y aplicaciones.

- Soporte técnico para atención de incidentes / problemas vía una mesa de servicios con herramientas adecuadas para control y seguimiento de casos con apego a la metodología ITIL (*Information Technology Infrastructure Library)* versión 3 como mínimo.
- Cambios de configuraciones, actualizaciones, alta de nuevas funcionalidades.

- Considerar en su propuesta la capacitación (operación y administración) que será ofrecida al personal que la DGTI designe (al menos 3 personas), en cada una de las soluciones que integren su propuesta, respecto de las marcas ofertadas en la solución de seguridad y en la solución de balanceo.

3. CARACTERÍSTICAS

- Arrendamiento "llave en mano", sin opción a compra, de una solución de seguridad perimetral mediante un contrato abierto que incluya hardware nuevo, servicios y software, de tecnología reciente, en una plataforma de seguridad que integre la infraestructura y los servicios especializados de soporte.
- La solución integral ofertada deberá cumplir con las especificaciones técnicas establecidas en el presente anexo. Las descripciones que se enuncian en este documento, relativas a componentes, especificaciones técnicas y requerimientos específicos de los equipos y servicios que forman parte del arrendamiento son las mínimas requeridas, por lo que solamente se aceptarán propuestas con especificaciones iguales o superiores a las solicitadas. La DGTI calificará como equivalente o superior la tecnología ofertada en base a la documentación aportada para su demostración y la verificación con los fabricantes o especialistas de terceros que pueda consultar.
- Servicios de implementación, migración de servicios actuales, integración a la infraestructura actual de red y soporte técnico especializado.
- Todo el Hardware y el Software deberán ser nuevos de la versión más reciente y con soporte dentro de la República Mexicana, se deberá presentar una carta firmada por el representante legal del licitante de que los productos ofertados cumplen con lo solicitado en este párrafo.
- El licitante deberá presentar una carta firmada por su representante legal donde se compromete a entregar, en caso de ser adjudicado, cartas firmadas por el fabricante que lo reconoce como distribuidor autorizado y que brindará el soporte y garantía en todos y cada uno de los componentes de la marca ofertada durante la vigencia del contrato.
- En caso de que el licitante resulte adjudicado, deberá exhibir una carta firmada por el representante legal del fabricante y dirigida el INAI (una carta por cada fabricante de cada producto), en donde lo acredite como distribuidor autorizado y que además brindará el soporte y garantía en todos y cada uno de los componentes de la marca ofertada durante la vigencia del contrato. Estas cartas deberán ser entregadas a mas tardar 3 días hábiles posteriores a la notificación del fallo. En caso de no entregar las cartas, se rescindirá en contrato.
- Toda la información transferida a través del Hardware o contenida en este, será propiedad del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

- El proveedor deberá proporcionar, el hardware, software y servicios especializados de soporte necesarios para la correcta implementación de la solución ofertada durante la vigencia del contrato.
- El proveedor deberá presentar una garantía o contrato de soporte vigente del fabricante en todos los componentes que integran la solución, mediante el cual el proveedor respaldará el correcto funcionamiento de los equipos, la cual aplicará durante la vigencia del contrato. Este documento deberá ser entregado 10 habiles días posteriores al inicio del contrato.
- Servicio de diagnóstico proactivo, actualizaciones de software y de microcódigo de la plataforma durante la vigencia del contrato.

  El licitante deberá considerar como parte de su propuesta un recurso certificado para asegurar la continuidad operativa del negocio (Business Continuity Management o BCM por sus siglas en inglés) el cual deberá poder asesorar cuando sea necesario al administrador del contrato para validar la correcta funcionalidad del plan de recuperación de desastres (Disaster Recovery Plan o DRP por sus siglas en inglés) en cuanto a políticas de seguridad. Para lo cual se deberá incluir un recurso para un promedio de 5 horas al mes.
- El proveedor deberá proveer la capacitación formal para la administración, operación y tratamiento de incidentes de las plataformas propuestas avaladas por cada uno de los fabricantes de las marcas utilizadas en la solución de seguridad y en la solución de balanceo.

4. ALCANCE DEL ARRENDAMIENTO

El proveedor implementará una solución integral de seguridad en capas que mantenga disponible el tráfico que cursa por los enlaces a Internet, tanto de entrada como de salida, capaz de proteger las aplicaciones WEB de vulnerabilidades y ataques, y al mismo tiempo que mantenga y mejore el nivel de seguridad perimetral e interno a través de una solución de dispositivos nuevos para el control de accesos, protección de intrusos y ataques de nueva generación, así como el monitoreo de movimientos laterales para la detección y prevención de amenazas avanzadas. Esta solución deberá estar lista antes del 1 de enero del 2020 para la migración de los servicios que actualmente se ejecutan en otra infraestructura.

La solución propuesta deberá ofrecer los equipos por lo menos en cinco capas integrando para ello equipo físico y en una arquitectura redundante en las capas (1, 2, 3 y 4) para garantizar la continuidad en los servicios informáticos del INAI.

La solución deberá estar integrada como mínimo por los siguientes componentes por capa:

1) Capa 1.- Equipamiento redundante para balanceo de enlaces y balanceo global con opción de soportar funcionalidades de seguridad para protección de DNS (*Domain Name System*).
2) Capa 2.- Equipamiento redundante (Cluster Activo/Pasivo) para protección de aplicaciones web.
3) Capa 3.- Equipamiento redundante (Cluster Activo/Pasivo) para capa de Next Generation Firewall (NGFW) con funcionalidades de control de aplicación, VPN, URL Filtering, administración de políticas, identificación de usuarios, Anti-Virus, Anti-Bot, Anti-Spam, se deberá incluir una consola de administración para la solución,

consola de log´s y reporteo, en appliance físico y licenciamiento de hasta 200 VPN's para usuarios móviles.

4) Capa 4.- Equipamiento para capa de prevención y detección de intrusos de siguiente generación (IDPS), deberá incluir consola de administración.
5) Capa 5.- Equipamiento para capa de detección y protección contra amenazas avanzadas.
6) Licenciamiento VPN de hasta 200 usuarios móviles.
7) Licenciamiento para 10 unidades de protección avanzada para servidores.

No se aceptarán soluciones UTM (Unified Threat Management) debiendo ofertar los equipos donde se solicita Hardware para cada una de las capas a nivel físico.

Para cada una de las soluciones utilizadas en cada capa descrita con anterioridad, el licitante deberá adjuntarse a su propuesta técnica las fichas técnicas, manuales, URL's o cualquier documento técnico avalado por el fabricante de la marca ofertada, que acredite el cumplimiento de la característica o funcionalidad solicitada en el presente anexo técnico. Para cada especificación técnica o funcionalidad del equipo ofertado referida en el numeral 5, se deberá indicar el documento de referencia, capitulo y/o núm. de página, la referencia deberá estar subrayada para pronta localización.

Funcionalidad	Descripción
Hardware para Balanceo de Tráfico de internet	• Balanceo dinámico de Tráfico • DNS autoritativo y reporteador de DNS.
Hardware para protección de aplicaciones WEB	• Ataques automatizados y bots. • Aplicación web y ataques de API. • Ataques de capa de aplicación. • Balanceador de aplicaciones. • Redireccionamiento HTTPS con soporte de reescritura.
Hardware para Seguridad Perimetral	• Firewall • URL Filtering • Application control • VPN • Identificación de Accesos de Usuarios • Anti-Virus, Anti-Bot, Anti-Spam
Hardware para solución de sistema de prevención, detección y protección de intrusos	• IDPS
Hardware para detección y protección contra amenazas avanzadas	• Ataques dirigidos y amenazas avanzadas • Aplicaciones disruptivas • Comportamiento del atacante y otras actividades de la red.
Servicio de protección avanzada para servidores	• Prevención de intrusos • Antimalware.

Funcionalidad	Descripción
	• Monitoreo e Integridad

Para fines del presente arrendamiento sin opción a compra de una solución de seguridad perimetral, se considera una sola partida como una solución integral "llave en mano" como se detalla más adelante en el presente documento.

Los equipos serán entregados al INAI a través dela DGTI, en sus instalaciones en la ciudad de México, sita en Insurgentes Sur Nº 3211, Col Insurgentes Cuicuilco, Alcaldía Coyoacán, CDMX C.P. 04530. La solución integral deberá estar instalada, configurada, puesta a punto y operando al 100% el 1 de enero de 2019.

La vigencia del contrato será del 1 enero de 2020 al 31 de diciembre de 2022.

Durante la instalación el proveedor debe garantizar la continuidad del servicio y en caso de incurrir en retrasos, o incurrir en la interrupción de cualquiera de los servicios durante la instalación, se aplicarán las penas convencionales que procedan. Se aceptarán interrupciones sobre ventanas de implementación mutuamente acordadas durante el proceso de instalación, configuración y puesta a punto de la solución.

5. DESCRIPCIÓN DE LOS EQUIPOS Y SERVICIOS REQUERIDOS.

5.1. ANTECEDENTES Y SITUACIÓN ACTUAL

Con objeto de asegurar la continuidad de los servicios de comunicaciones con la seguridad y alta disponibilidad que requiere la operación del INAI, se cuenta actualmente con un contrato que provee algunos de los servicios en el alcance del presente Anexo Técnico, mismo que terminará su vigencia el 31 de diciembre de 2019.

El INAI a través de la DGTI, requiere no solo la renovación de los servicios, sino también la renovación tecnológica e incorporación de nuevas funcionalidades con objeto de contar con una solución de última generación que asegure la disponibilidad del tráfico que cursa por los enlaces a Internet, tanto de entrada como de salida y al mismo tiempo que mantenga y mejore el nivel de seguridad, con control de accesos y protección de intrusos y ataques para amenazas de nueva generación, vulnerabilidades y protección de aplicaciones que han evolucionado con respecto a lo que se tenía hace por lo menos tres años.

5.2. CAPA DE HARDWARE DE BALANCEO DE TRAFICO DE INTERNET

La solución de alta disponibilidad con balanceo de carga de enlaces ofertada por el licitante, deberá ser capaz de mantener estable y al mismo tiempo optimizar la operatividad del tráfico de datos que cursa por los dos enlaces dedicados a Internet que posee el INAI, conforme a sus prioridades y capacidades de consumo del ancho de banda. El instituto cuenta actualmente con 2 enlaces a Internet, con capacidades mínimas de 150 Mbps cada uno y con capacidad de crecimiento durante la vigencia del contrato.

Con base a lo anterior, el licitante deberá ofertar la infraestructura (hardware y software) necesaria para asegurar el poder brindar el balanceo de carga sobre los enlaces a Internet para entrada / salida en alta disponibilidad. Por lo que deberá considerar en su solución propuesta como mínimo 2 equipos físicos en Alta disponibilidad (High Availability - HA).

Los equipos / componentes de la solución propuesta deberán cumplir como mínimo con los siguientes requerimientos:

Hardware:

- ✓ Los equipos ofertados deberán ser bajo una plataforma de hardware de propósito específico denominado "hardware" con software propiedad del mismo fabricante del Hardware, no se aceptarán soluciones de SW integradas en servidores de terceros.
- ✓ Throughput Nominal mínimo de 6 Gbps para balanceo en condiciones de máxima carga.
- ✓ La solución debe soportar un Throughput en L7 (Capa 7) y L4 (Capa 4) de 10 Gbps por cada hardware.
- ✓ La solución debe soportar al menos 5 Millones de conexiones concurrentes en total por cada hardware.
- ✓ La solución debe soportar al menos 14 millones conexiones por segundo en L4 (Capa 4) por cada hardware.
- ✓ Interfaces de red:
  - ✓ Debe soportar al menos 4 puertos de Gigabit Ethernet en SFP en cobre.
  - ✓ Opción para soportar 2 puertos de Fibra Óptica a 10 Gbps para crecimiento.
- ✓ Contar con Fuentes de poder redundantes AC, entradas de voltaje de 220 VAC que se puedan remover en caliente (hot-swap) con cable con conector nema C14.
- ✓ Los equipos deberán estar habilitados para ser instalados en rack estándar de 19".
- ✓ Los equipos deberán ser configurados en alta disponibilidad, es decir, tener la capacidad de conectarse a una unidad similar y operar en modo activo con la otra unidad en modo pasivo (fail-over) y deberá contar con la capacidad de direccionamiento virtual. El esquema debe tener la capacidad para recuperación de las sesiones del sistema en forma inmediata y automática en caso de fallo de un adaptador, cable de red, canal de controladora o alimentación de fluido eléctrico.
- ✓ Debe poder soportar configuración en cluster Activo/Activo entre dos o más plataformas. (Las plataformas adicionales no necesariamente tendrán que ser del mismo modelo)
- ✓ Los equipos deberán contar con memoria RAM mínimo de 16 Gb por hardware y contar mínimo con un Disco duro de 500 Gb por hardware.
- ✓ Si existe la necesidad de conmutar el tráfico a otro dispositivo del grupo, el sistema deberá poder realizar cálculos para determinar el mejor dispositivo basado en: recursos, capacidad, carga de tráfico en cada dispositivo. Identificando la mejor opción cuando el ambiente sea heterogéneo en cuanto se refiere a plataformas
- ✓ Deberá manejar compresión por Hardware de al menos 4 Gbps y no se aceptará compresión por software.
- ✓ La configuración deberá poder ser sincronizada entre todos los dispositivos del grupo, permitiendo optar por sincronización automática o manual.

Software:

- ✓ El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante específicamente para las funciones de balanceo de tráfico entrante y saliente hacia y desde múltiples ISP's (*Internet service provider*) siendo estos de diferentes capacidades y diferentes proveedores. Todo lo anterior deberá demostrarse que se efectúa sin la necesidad de utilizar BGP (*Border Gateway Protocol*).
- ✓ La solución debe realizar funciones de balanceo de tráfico entrante y saliente hacia y desde múltiples ISP's.
- ✓ Deberá tratarse de una herramienta que soporte algoritmos de automatización como podrían ser Universal Inspection Engine, iRules, scripts, equivalentes o superiores que permita examinar todo el payload o header de la aplicación, ya que esta tecnología es la que se usa actualmente y se cuenta con perfiles que deberán ser migrados funcionalmente al 100% a la plataforma nueva (En caso de no poder migrar las reglas

en tiempo, el proveedor está obligado a prestar el servicio y deberá conservarse el mismo con algún equipo temporal a fin de no poner en riesgo la operación del INAI).

- ✓ La solución debe tener arquitectura Full-Proxy, control de entrada y salida de conexiones distinguiendo conexiones del lado del cliente y del lado del servidor o los recursos
- ✓ Deberá contar con la capacidad de mantener persistencia en las sesiones, asegurando que un usuario siempre sea balanceado a través del mismo ISP, a menos que haya una falla en el enlace.
- ✓ Deberá contar con monitores predefinidos y personalizables que permiten comprobar y verificar la salud y disponibilidad de cada componente del enlace (velocidad, tiempo respuesta, costo, etc.)
- ✓ Deberá contar con la capacidad de L7 rate shaping.
- ✓ Deberá soportar la capacidad de agregar software que suministre funcionalidades como compresión selectiva (en base a tipo de contenido y cliente) de datos (http), Gateway IPV6. Todo esto sin la necesidad de agregar hardware adicional
- ✓ Deberá tener la capacidad de agregar funcionalidades al equipo sin necesidad de apagarlo o intervenirlo físicamente.
- ✓ Deberá contar con métodos de balanceo de carga estático y dinámico, con garantía de mantenimiento de sesión entre sistemas redundantes.
- ✓ Deberá permitir el balanceo dinámico basado en los siguientes atributos de link
  - ✓ Ancho de Banda disponible en el link
  - ✓ Costo de Ancho de Banda adquirido.
  - ✓ Capacidad de Link y límite de recursos (Inbound)
  - ✓ Capacidad de Link y límite de recursos (Outbound)
- ✓ Deberá contar con la capacidad de Balanceo basado en Tipo de Servicio (ToS) y Calidad de servicio (QoS).
- ✓ Deberá asegurar la continuidad, seguridad y rendimiento correcto al interceptar, inspeccionar, transformar, y dirigir las solicitudes de las aplicaciones y los servicios Web basándose en valores encontrados en cualquier punto del paquete o "Payload" (tener capacidad de abrir el payload completo y tomar decisiones en base a cualquier tipo de contenido).
- ✓ Deberá soportar las funcionalidades completas para tener el roll de DNS autoritativo.

Red:

- ✓ Deberá contar como mínimo con:
  - ✓ Soporte VLAN 802.1q, Vlan tagging
  - ✓ Soporte de 802.3ad para definición de múltiples troncales
  - ✓ Soporte de NAT, SNAT
    - ✓ Soporte de IPv6: El equipo debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente.
  - ✓ Soporte de Rate Shapping.
  - ✓ Soporte de dominios de Enrutamiento, donde cada uno pueda tener su propio Default Gateway y estar conectados a redes IP con el mismo direccionamiento.

Consola de Administración

- ✓ La solución debe permitir el acceso para la administración del equipo hardware vía CLI (Interfaz de línea de comandos) por SSH, interfaz de administración gráfica basada en Web seguro (HTTPS)
- ✓ La solución deberá poder integrarse con Directorio Activo Windows 2003 o superior, LDAP, RADIUS.

- ✓ La solución debe incluir comunicación cifrada y permitir la autenticación del equipo y de los usuarios administradores/supervisores con Certificados Digitales
- ✓ La solución debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante:
  - ✓ Protocolo SysLog
  - ✓ Notificación vía SMTP
  - ✓ SNMP versión.2.0 o superior.
- ✓ El sistema de administración debe ser totalmente independiente del sistema de procesamiento de tráfico.
- ✓ El equipo debe contar con un módulo de administración tipo lights out que permita encender/apagar el sistema de manera remota y visualizar el proceso de arranque.
- ✓ La interfaz gráfica debe contar con un Dashboard personalizable que permita monitorear el estado del equipo en tiempo real
- ✓ Debe contar con un módulo de reportes que permita visualizar gráficamente el comportamiento de las aplicaciones HTTP como latencias hacia los servidores, latencias en los URL, Direcciones IP que acceden las aplicaciones, las URL más visitados en las aplicaciones, Throughput hacia los servidores y estadísticas acerca de los servicios creados y los servidores físicos.

5.3. CAPA DE HARDWARE PARA PROTECCIÓN DE APLICACIONES WEB

La solución ofertada deberá constar de una plataforma de hardware de propósito específico denominado "appliance", para uso específico como WAF (*Web Application Firewall*), la solución deberá estar conformada de por lo menos dos equipos en Alta disponibilidad (High availability - HA)

La solucione debe contener como mínimo más no limitativo las siguientes características:

- ❖ Hardware
  - ✓ Deberá cumplir con las siguientes características:
    - o La solución debe soportar un Throughput en L4 de al menos 20 Gbps.
    - o La solución debe soportar un Throughput en L7 de al menos 20 Gbps.
    - o La solución debe soportar al menos 28 Millones de conexiones simultáneas.
    - o La solución debe soportar al menos 450.000 conexiones por segundo en L4.
    - o La solución debe soportar al menos 2 Millon de HTTP Requests por Segundo.
    - o Al menos 4 puertos SFP+, con opción de conectividad de 1 Gbps en cobre.
    - o Al menos 2 puertos SFP+, con opción de conectividad de 10 Gbps en fibra.
    - o Los equipos deberán ser instalados en rack estándar de 19", máximo 2RU.
    - o Cada equipo debe incluir 32 Gb de Memoria RAM mínimo.
    - o Cada equipo debe incluir mínimo un Disco duro de 500 Gb.
    - o Contar con Fuentes de poder redundantes AC, entradas de voltaje de 220 VAC que se puedan remover en caliente (hot-swap) con cable con conector nema C14.
    - o
- ❖ Software
  - ✓ El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante específicamente para propósitos de Firewall de aplicaciones WEB
    - ▪ La solución deberá contar con características de balanceo de carga de Servicios, aplicaciones basadas en IP(TCP/UDP) y servicios WEB.

- La solución debe poder balancear la carga en los servidores back-end con mínimo los siguientes algoritmos de balanceo: round robin, menor conexión, respuesta más rápida.
- Soporte redireccionamiento http a https con rewriting.
- Balanceador de aplicaciones
- Reporteador en línea del comportamiento de los ataques, reputación, geolocalización. Además, del tráfico de las aplicaciones

❖ Red
- ✓ Deberá cumplir con los siguientes estándares de red:
  - o Soporte VLAN 802.1q, Vlan tagging.
  - o Soporte de 802.3ad para definición de múltiples troncales.
  - o Soporte de NAT, SNAT.
  - o Soporte de IPv6: El equipo debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente.
  - o Soporte de Rate Shapping.
  - o Soporte de dominios de Enrutamiento, donde cada uno pueda tener su propio Default Gateway y estar conectados a redes IP con el mismo direccionamiento.
  - o Debe soportar redes virtuales, Gateways virtuales, NVGRE y Transparent Ethernet Bridging para entornos de redes virtualizadas.

❖ Seguridad perimetral
- ✓ Deberá cumplir con las siguientes características de seguridad perimetral:
  - o Soportar seguridad SSL con las siguientes características
    - o Incluir el soporte de Aceleración SSL usando Hardware Dedicado
    - o Incluir mínimo 20,000 Transacciones por segundo SSL (RSA 2K Keys).
    - o Incluir mínimo 10,000 Transacciones por segundo SSL (ECDSA P-256).
    - o Soportar al menos 15 Gbps SSL Bulk Encryption (Thoughput SSL).
    - o Soporte de llaves SSL RSA de 1024, 2048 y 4096 bits.
  - o El Stack TLS del equipo debe soportar las siguientes funcionalidades/características
    - o Session ID
    - o Session Ticket.
    - o OCSP Stapling (on line certificate status protocol).
    - o Dynamic Record Sizing.
    - o ALPN (Application Layer Protocol Negotiation).
    - o Forward Secrecy.
  - o La solución debe manejar AES, AES-GCM, SHA1/MD5 y soporte a algoritmos de llave pública: RSA, Diffie-Hellman, Digital Signature Algorithm (DSA) y Elliptic Curve Cryptography (ECC).
  - o La solución debe permitir la funcionalidad Proxy SSL, esta funcionalidad permite que sesión SSL se establezca directamente entre el usuario y el servidor final, sin embargo, el equipo debe ser capaz de desencriptar, optimizar y Re encriptar el tráfico SSL sin que termine la sesión SSL.

❖ Seguridad aplicativa
- ✓ Deberá cumplir con las siguientes características de seguridad aplicativa:
  - o La solución debe poder realizar la comprobación de estado a nivel de la aplicación de los servidores backend.

- La solución debe poder admitir el almacenamiento en caché y la compresión hasta de 5 Gb en una sola plataforma.
- La solución debe permitir el paso del tráfico cuando fallan los servicios.
- El WAF debe poder admitir la configuración de vlan a través de un switch incorporado.
- La solución debe poder realizar la optimización TCP / IP.
- La solución debe poder realizar el filtrado de paquetes.
- La solución debe ser compatible con TLS1.0, TLS1.1, TLS1.2 y TLS1.3.
- La solución debe admitir una curva elíptica de módulo primario de 384 bits.
- La solución debe ser compatible con HTTP Strict Transport Security Support (HSTS) recomendado por las prácticas recomendadas de implementación de SSL Labs.
- La solución debe admitir la función SSL de proxy que permite que el cliente se autentique directamente con el servidor y el servidor para autenticar al cliente según el certificado del cliente presentado.
- La solución debe proporcionar seguimiento de sesión con capacidades mejoradas de generación de informes y cumplimiento que toman en cuenta las sesiones de usuario HTTP y los nombres de usuario de la aplicación dentro de la aplicación. Esto le brinda al administrador más información sobre actividades sospechosas de la aplicación (por ejemplo, quién fue el usuario detrás de un ataque) y más flexibilidad para aplicar la política de seguridad (como impedir que un determinado usuario use la aplicación). Se puede configurar si el sistema realiza un seguimiento de las sesiones según el nombre de usuario, la dirección IP o el número de identificación de la sesión.
- El WAF debe proporcionar un registro integrado a sistemas de seguimiento de eventos de seguridad de terceros, como SIEM.
- El WAF debe proporcionar el siguiente soporte HTTP / HTML
  - El WAF debe ser compatible con las versiones HTTP 1.0 y 1.1 o versiones superiores cuando estén disponibles en el mercado
  - El WAF debe ser compatible con la codificación de aplicación / x-www-form-urlencoded
  - El WAF debe admitir v0 cookies o versiones superiores a medida que estén disponibles en el mercado.
  - El WAF debe admitir las cookies v1 o versiones superiores a medida que estén disponibles en el mercado.
  - El WAF debe hacer cumplir los tipos de cookies utilizados
  - El WAF debe admitir la codificación fragmentada en las solicitudes
  - El WAF debe admitir la codificación fragmentada en las respuestas
  - El WAF debe soportar la compresión de solicitud
  - El WAF debe soportar compresión de respuesta
  - El WAF debe admitir la administración de flujos de aplicaciones y definir manualmente el flujo del sitio y las políticas de objetos
  - El WAF debe soportar todos los juegos de caracteres durante la validación
  - El WAF debe restringir los métodos utilizados, por ejemplo, GET, POST, todos los demás métodos
  - El WAF debe restringir los protocolos y las versiones de protocolo utilizadas.
  - El WAF debe admitir la codificación de idiomas de múltiples bytes
  - El WAF debe validar los caracteres codificados en URL
- El WAF debe admitir las siguientes técnicas de detección evasiva

- Decodificación de URL
- Terminación de cadena de bytes nulos
- Rutas de autorreferencia (es decir, uso de /./ y equivalentes codificados)
- Referencias de ruta (es decir, uso de /../ y equivalentes codificados)
- Caso mixto
- Uso excesivo de espacios en blanco
- Eliminación de comentarios (por ejemplo, convertir BORRAR / ** / DE a BORRAR DE)
- Conversión de caracteres de barra invertida (compatibles con Windows) en caracteres de barra diagonal.
- Conversión de codificación Unicode específica de IIS (% uXXYY)
- Decodifique las entidades HTML (por ejemplo, c, & quot ;, & # xAA;)
- Caracteres escapados (por ejemplo, \ t, \ 001, \ xAA, \ uAABB)

- El WAF debe admitir las siguientes técnicas de detección evasiva:
  - Decodificación de URL
  - Terminación de cadena de bytes nulos
  - Rutas de autorreferencia (es decir, uso de /./ y equivalentes codificados)
  - Referencias de ruta (es decir, uso de /../ y equivalentes codificados)
  - Caso mixto
  - Uso excesivo de espacios en blanco
  - Eliminación de comentarios (por ejemplo, convertir BORRAR / ** / DE a BORRAR DE)
  - Conversión de caracteres de barra invertida (compatibles con Windows) en caracteres de barra diagonal.
  - Conversión de codificación Unicode específica de IIS (% uXXYY)
  - Decodifique las entidades HTML (por ejemplo, c, & quot ;, & # xAA;)
  - Caracteres escapados (por ejemplo, \ t, \ 001, \ xAA, \ uAABB)
- El WAF debe poder protegerse contra
  - Entrada no validada
  - Defectos de inyección
  - inyección SQL
  - Inyección OS
  - Manipulación de parámetros
  - Envenenamiento con cookies
  - Manipulación de campos ocultos
  - Fallas de secuencias de comandos de sitio
  - Desbordamientos de búfer
  - Control de acceso roto
  - Autenticación rota y gestión de sesión
  - Manejo inadecuado de errores
  - Bombas XML / DOS
  - Navegación forzada
  - Fuga de información sensible.
  - Secuestro de sesión
  - Negación de servicio
  - Solicitud de contrabando
  - Manipulación de cookies

❖ Consola de Administración

- ✓ Deberá cumplir con las siguientes características de seguridad aplicativa:
  - La solución debe permitir el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH, interfaz de administración gráfica basada en Web seguro (HTTPS).
  - La solución debe integrarse con Directorio Activo Windows 2003 o superior, para la autenticación de usuarios para gestión de la herramienta.
  - La solución debe integrarse con LDAP, para la autenticación de usuarios para gestión de la herramienta.
  - La solución debe integrarse con RADIUS y TACACS+ para la autenticación de usuarios para gestión de la herramienta.
  - La solución debe incluir comunicación cifrada y permitir la autenticación del equipo y de los usuarios administradores/supervisores con Certificados Digitales.
  - Debe contar con un módulo de reportes que permita visualizar gráficamente el comportamiento de las aplicaciones HTTP como latencias hacia los servidores, latencias en los URL, Direcciones IPs que acceden las aplicaciones, URLs más visitados en las aplicaciones, Throughput hacia los servidores y estadísticas acerca de los servicios creados y los servidores físicos.
  - La solución debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante:
    - Protocolo SysLog
    - Notificación vía SMTP
    - SNMP versión.2.0 o superior.

El equipo o sistema operativo debe estar certificado por ICSA Labs como Firewall de Red (Corporate Firewall).

5.4. CAPA DE HARDWARE SEGURIDAD PERIMETRAL

El licitante deberá proponer como alcance de su oferta, la infraestructura (hardware y software) necesaria para cubrir la funcionalidad de seguridad perimetral (firewall) realizando el control de acceso en alta disponibilidad.

La solución de hardware para seguridad perimetral (Firewall) ofertada deberá contar como mínimo con las siguientes características y funcionalidades:

Características generales

- ✓ Se deberá ofertar una solución de por lo menos dos equipos en equipos en Alta disponibilidad (High availability - HA) del tipo NGFW.
- ✓ La solución deberá contar con la última versión de S.O. del fabricante y se deberán ofertar las actualizaciones liberadas por el fabricante durante los tres años del servicio incluidas en la propuesta presentada.
- ✓ La solución deberá permitir crear controles de acceso a aplicaciones / servicios / protocolos predefinidos mediante servicios de filtrado web/URL.
- ✓ La solución deberá proteger implementaciones de VoIP, soportando H323, SIP. MGCP y SCCP.
- ✓ La solución incluir la posibilidad de crear NATs dinámicos (N-1) y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete y en una sola regla.
- ✓ La solución propuesta deberá contar con una consola centralizada, capaz de administrar los Firewall propuestos, la cual deberá ser una consola fisica de appliance

del mismo fabricante con la capacidad de almacenamiento de logs necesaria y esta no deberá de ocupar más de dos unidades de rack.

- ✓ Dicha consola debe permitir la gestión de políticas con el monitoreo y la gestión de eventos en un dispositivo dedicado de alto rendimiento.

Hardware

- ✓ El equipo deberá garantizar al menos 28 Gbps de desempeño reales en Firewall
- ✓ El equipo deberá tener al menos 8 interfaces 10/100/1000 RJ45
- ✓ El equipo deberá contar con al menos 4 interfaces SFP 10 Gbps SR las que deberán entregarse en fibra con sus respectivos jumpers.
- ✓ El equipo deberá garantizar al menos 9.5 Gbps en desempeño VPN en AES-128
- ✓ El equipo deberá garantizar al menos 190,000 conexiones por segundos
- ✓ El equipo deberá garantizar a máxima capacidad de memoria 10,500,000 conexiones concurrentes
- ✓ Dicha solución debe ser sumamente flexible, permitiendo que se añadan nuevos bloques de seguridad sin la necesidad de agregar nuevo hardware/software o complejidad a la administración (esto es que permita activar módulos o características de seguridad del Sistema Operativo que cubran los requerimientos solicitados sin que para ello se requiera hacer la modificación del hardware ofertado)
- ✓ El equipo deberá venir equipado con al menos 2x480 GB de almacenamiento local contra fallas con la finalidad de garantizar la preservación de las bitácoras y logs generados por el mismo equipo, como por ejemplo el arreglo de discos RAID1.
- ✓ Contar con Fuentes de poder AC, entradas de voltaje de 220 VAC con cable con conector nema C14.Software:
- ✓ Con el fin de mantener la segmentación de la red, el equipo debe ser capaz de virtualizar como mínimo 20 sistemas adicionales (Virtuales) de firewalls
- ✓ Debe tener la opción de negar los parámetros de origen o destino, es decir que para una regla dada permite todas las conexiones de origen / destino excepto la especificada en la regla
- ✓ Debe permitir implementar reglas aplicadas a intervalos de tiempo específicos
- ✓ La comunicación entre los servidores de administración y los gateways, debe ser cifrada y autenticadaDebera cumplir con alguno de los siguientes esquemas de autenticación en los módulos de firewall y VPN: tokens (por ejemplo, SecureID), TACACS, RADIUS, certificados digitales
- ✓ Debe permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo
- ✓ Debe ser compatible con Active Directory.
- ✓ El firewall debe poder conectarse modo transparente (transparent mode)
- ✓ Debe permitir el controlar el acceso a archivos compartidos de Microsoft usando CIFS.
- ✓ Debe tener equipado lo necesario para tener Alta Disponibilidad, incluyendo la licencia para Alta Disponibilidad.
- ✓ La consola de administración del firewall, deberá proporcionar una visión clara del cumplimiento de múltiples regulaciones necesarias para las operaciones del INAI (ISO 27001 e ISO 27002) a través del monitoreo de las políticas de seguridad en una sola vista.
- ✓ El fabricante de la solución propuesta debe haber estado catalogado como líder en el cuadrante de Gartner en la categoría de Enterprise Network Firewalls como mínimo durante los últimos 3 años.
- ✓ El fabricante de la solucion propuesta debe estar recomendado por NSS Labs en la categoría de NeXT Generation Firewall en el 2018 arriba del 95 % de efectividad.

- ✓ El fabricante debe estar certificado por ICSA Labs en su versión actual al menos desde hace 2 años.

Red:

- ✓ El Gateway debe soportar redundancia a enlaces, sin la necesidad de una licencia adicional o software / Hardware de terceros.
- ✓ Generación de políticas L3, L4 y L7.
- ✓ Soporte IPv4 y v6.
- ✓ Soporte Static NAT
- ✓ NAT with Port Translation
- ✓ Soporte de 802.1.q

Filtrado Web equipado dentro del NGFW.

- ✓ Deberá contar con la capacidad de integrarse con Servidores de Autenticación Microsoft Windows Active Directory o LDAPv3 permitir la creación de políticas de acceso basadas en identidad en la política de seguridad del Next Generation Firewall para acceso a usuarios y/o grupos de usuarios para el uso de las aplicaciones y los sitios Web que les sean autorizados
- ✓ Deberá contar con la capacidad de interactuar con los controladores de Dominio de Active Directory sin requerir algún tipo de agente a ser instalado
- ✓ Deberá brindar políticas de seguridad unificadas para el control de aplicaciones y URLF, donde estas contarán con la capacidad de poder manejar múltiples categorías en una misma política.
- ✓ Deberá contar con la capacidad de identificar aplicaciones a partir de la inspección del tráfico que cruce la solución en forma independiente del puerto y protocolo hacia el cual esté utilizando.
- ✓ Deberá contar un listado de al menos 2500 aplicaciones ya definidas por el fabricante para control de aplicaciones, donde esta lista pueda ser validada con información pública del fabricante y contar con una categorización de sitios Web que exceda 200 Millones de URL y que permita brindar el factor de Riesgo
- ✓ Deberá brindar actualizaciones periódicas y automatizadas hacia la infraestructura, donde las aplicaciones identificadas deberá contar con la capacidad para definir al menos las siguientes opciones de control: Permitir, Informar y Bloquear registrando cada uno de los accesos en las bitácoras. Por otro lado, para aplicaciones no identificadas (desconocidas) deberá contar con la capacidad para definir al menos las siguientes opciones: Permitir, Informar y Bloquear registrando cada uno de los accesos en las bitácoras
- ✓ Deberá contar con la capacidad de crear políticas granulares para sitios Web, Web 2.0
- ✓ Deberá contar con la capacidad de crear políticas granulares por aplicación, en especial aplicaciones P2P, indicando la limitación de ancho de banda por tipo de aplicativo o bien por grupos
- ✓ Deberá contar con capacidad de inspección paralela para tráfico HTTPS/SSL con el fin de controlar las aplicaciones y prevenir riesgos de seguridad, permitiendo la posibilidad de crear políticas granulares indicando en que categorías se realizara inspección y cuales se permitirá bypass para que no sea inspeccionado
- ✓ Deberá notificar en idioma español al usuario final la indicación de incumplimiento de la política de Navegación Segura definida por el INAI a través de la DGTI.

Deberá venir equipado con lo necesario para implementar el control de accesos de usuarios conforme a lo que se acuerde en el plan de trabajo durante la vigencia de los servicios con el Administrador del contrato.

VPN:

El licitante deberá proponer la infraestructura (hardware y software) para permitir acceso remoto de al menos 100 y hasta 200 usuarios móviles a través de VPN a recursos internos de la red de la organización, la solución propuesta debe ser ofertada en alta disponibilidad y debe estar contenida como un servicio licenciado dentro de la plataforma del Firewall.

Las características y funcionalidades mínimas requeridas son las siguientes:

- ✓ Deben ser soportadas tanto una CA Interna como una CA externa provista por un tercero.
- ✓ Deben ser soportados 3DES y AES-256 para las fases I y II de IKE
- ✓ Con el fin de soportar un máximo nivel de cifrado se deben soportar los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit), Grupo 19 (256-ECP) y Grupo 20 (384-ECP)
- ✓ Con el fin de asegurar la máxima integridad de datos se deben soportar los esquemas: MD5, SHA1 y SHA384.
- ✓ Debe permitir topologías VPNs site-to-site: Full Meshed (todos a todos), Star (Oficinas Remotas a Sitio Central) y Hub and Spoke (Sitio remoto a través del sitio central hacia otro sitio remoto)
- ✓ Debe manejar VPNs client-to-site basadas en IPSEC.
- ✓ Debe tener la posibilidad de realizar VPNs SSL sin cliente para acceso remoto, sin necesidad de instalar un cliente
- ✓ Con el fin de evitar la conexión mediante VPN de dispositivos no confiables, la solución debera ser configurada para detectar y evitar la conexión de terminales móviles cuando estos sean vulnerados mediante técnicas de escalación de privilegios como pudieran ser jailbroken (iOS) y rooting (Android)
- ✓ Debe incluir un método simple y central, de crear túneles permanentes entre gateways del mismo fabricante
- ✓ Debe soportar VPNs tipo "domain based" y/o AD y "route based", usando al menos BGP y OSPF
- ✓ Debe incluir un mecanismo para mitigar el impacto a ataques de denegación de servicio DoS a IKE, haciendo diferencia entre conexiones conocidas y desconocidas
- ✓ Debe poder establecer VPNs con gateways con direcciones IP dinámicas públicas
- ✓ Debe manejar compresión IP para VPNs client-to-site y site-to-site.
- ✓ Debe ser posible crear una única asociación de seguridad (equivalente o superior) por par de redes o subredes.
- ✓ La solución debe contar con un mecanismo que permita seleccionar qué enlace utilizar para tráfico de VPN entrante y saliente, además de escoger la mejor ruta para dicho tráfico
- ✓ La solución debe tener la posibilidad de establecer VPN's sitio a sitio con IP dinámicas

5.5. CAPA DE HARDWARE PARA SOLUCIÓN DE SISTEMA DE PREVENCIÓN, DETECCIÓN Y PROTECCIÓN DE INTRUSOS.

El licitante deberá proponer como alcance de su oferta, la infraestructura (hardware/software) necesaria para cubrir la funcionalidad de la capa de detección de intrusos a nivel de red (IDPS de red) con control de tráfico por reputación dentro de la funcionalidad misma ofertada en la solución. Lo anterior mediante dos equipos de propósito específico que serán colocados dentro de la infraestructura de seguridad del Instituto. La

solución de prevención y detección de intrusos deberá ser de nueva generación en Sistemas de prevención y detección de intrusos (IDPS). La solución también podrá ser configurada en alta disponibilidad (activo – activo o Activo – pasivo) si el Instituto así lo requiere por lo cual los equipos ofertados en la solución deberán poder soportar dicha configuración sin necesidad de hardware o software adicional.

La solución IDPS deberá ser basada en Hardware para realizar inspección profunda ya que no se aceptarán soluciones basadas en hardware y software de propósito común, el IDPS deberá tener la capacidad de inspeccionar los paquetes de capa 2 a capa 7 del modelo OSI sin afectar el desempeño de la red.

La solución de protección contra ataques de nueva generación (IDPS) ofertada deberá contar como mínimo con lo siguiente:

Características y funcionalidades:

- ✓ El licitante deberá proponer un equipo IDPS dedicado basado en hardware de propósito específico, no se aceptan equipos multifuncionales (UTM) con módulos de IDPS activados, así mismo la solución debe incorporar baja latencia para obtener un mejor desempeño y escalabilidad y ser invisible a nivel de dirección IP al operar en línea.
- ✓ El IDPS propuesto debe tener habilitada la inspección de respuestas HTTP y esto no debe degradar el desempeño del equipo, siendo posible configurar el modo de procesamiento de análisis de respuestas HTTP.

Hardware:

- ✓ El IDPS debe ser una plataforma modular de uso especifico para IDPS (No se aceptarán NGFW's u otros UTM's emulando funciones de IPS) contando con al menos 2 ranuras para integrar diferentes módulos de puertos para interfaces de red de 1Gbps en cobre, 1Gbps en fibra, 10 Gbps en fibra SR, 10 Gbps en fibra LR.
- ✓ El licitante debe proponer 2 equipos IDPS que puedan operar en esquema stand alone o esquema de Alta disponibilidad; cada uno con las siguientes características de desempeño:
  - ✓ La solución deberá soportar hasta como mínimo 5 Gigas de inspección por cada caja y tener la capacidad de crecimiento de inspección de cuando menos 4 veces sin necesidad de hardware adicional. Es decir que cuando INAI solicite un crecimiento únicamente deberá licenciarse la capacidad adicional y no tener que cambiar de HW.
  - ✓ Incluir 12 puertos 1GbE en cobre para inspección de 6 segmentos de red en línea para cada caja.
  - ✓ Incluir 8 puertos 10GbE SR en fibra para inspección de 4 segmentos de red en línea por cada caja.
  - ✓ Deberá tener documentada una latencia menor a 40 micro segundos.
- ✓ El equipo IDPS no debe exceder las 2 unidades de rack por caja para garantizar que cabe en el espacio designado en el centro de datos.
- ✓ La solución debe soportar esquemas de alta disponibilidad Activo-Pasivo y Activo-Activo en donde 2 equipos estén sincronizados y en caso de falla de alguno de ellos los servicios de inspección no sean interrumpidos. Los equipos deben sincronizar al menos información sobre flujos bloqueados, flujos con control de ancho de banda (rate-limit), flujos en cuarentena.
- ✓ Deberá tener la capacidad de ser implementado en HA sin sacrificar desempeño en caso de falla de alguno de los Appliances, para lo que se deberá entregar documentación emitida por parte de un tercero como NSS LAB que avale que la familia

del IDPS cumple las características anunciadas por el fabricante. Esta documentación no podrá ser mayor a cuatro años.

- ✓ Contar con Fuentes de poder redundantes AC, entradas de voltaje de 220 VAC que se puedan remover en caliente (hot-swap) con cable con conector nema C14.
- ✓ Funcionalidad de bridge transparente inspeccionando en línea sin necesidad de IP.
- ✓ La arquitectura de solución propuesta deberá garantizar mediante las Alta disponibilidad y la inspección de segmentos propuesta que en caso de falla de alguna de las cajas existirá una segunda operando que garantice la inspección de los segmentos hasta en tanto se recupere la fallida.
- ✓ En caso de que llegase a existir falla simultanea de ambas unidades se deberá contar con un mecanismo de bypass, a fin de no interrumpir el flujo de paquetes de las aplicaciones sustantivas y las operativas de usuarios.
- ✓ Contar con Fuentes de poder redundantes AC, entradas de voltaje de 220 VAC que se puedan remover en caliente (hot-swap) con cable con conector nema C14.

Software:

- ✓ El fabricante del IDPS debe estar recomendado por NSS Labs en la categoría de NEXT Generation intrusion prevention system durante los últimos 2 años.
- ✓ El IDPS ofertado deberá ser capaz de operar y proteger ambientes en los cuales exista tráfico Asimétrico sin necesidad de realizar cambios a la topología de la red
- ✓ El IDPS propuesto debe contar con fuentes de poder redundante de tipo hotswap
- ✓ El proceso de Actualización del Sistema Operativo deberá tener la capacidad de ser aplicado con tráfico en vivo (sin necesidad de aplicar Bypass o que entre en función el equipo de HA en un cluster) y tener capacidad de poder seguir inspeccionando el tráfico sin afectación alguna durante la actualización.

Características de Seguridad

- ✓ Los filtros del IDPS deben soportar al menos las siguientes acciones de red: Block (bloqueo de paquetes), Block (reset TCP), Permit (permitir paquete), Trust (tráfico confiable), Notify (notificar), Trace (captura del paquete)
- ✓ Los filtros de la solución IDPS deben ser agrupados en categorías, para facilitar la administración contando con al menos las siguientes categorías: Exploits, Robo de Indentidad, reconocimiento, Política de Seguridad, Spyware, Virus, Vulnerabilidades, Equipos de red, Normalización de tráfico, mensajería instantánea, P2P y Streaming media
- ✓ La solución de IDPS propuesta debe tener el reconocimiento de la industria en descubrimiento de vulnerabilidades de día cero (Zero Day Vulnerability). Se deberá proporcionar una liga pública en donde se muestren las vulnerabilidades de día cero descubiertas por el centro de investigación de la solución propuesta indicando cuales han sido publicadas y cuales están pendientes de su revelación pública por parte de los correspondientes fabricantes de software.
- ✓ El IDPS deberá brindar protección contra ataques de día cero (nuevos ataques conocidos) y con la opción de contar con un sistema de monitoreo global reconocido para el manejo de este tipo de ataques a nivel mundial el cual debe ser referenciable públicamente para conocer la criticidad de los eventos que están ocurriendo en el mundo, así mismo deberá existir la opción de contar con un servicio que permita el acceso/consulta a una base de datos privada de vulnerabilidades, que permita ser personalizable.
- ✓ El IDPS deberá contar con la capacidad de realizar modelado de protocolo para analizar cualquier protocolo, existente y/o propietario sin necesidad de hacer actualizaciones al sistema operativo del IDPS.

Red:

- ✓ El IDPS propuesto debe ser capaz de soportar políticas de Seguridad granular, basado en los siguientes métodos:
  - ✓ Por dispositivo IDPS (todos los segmentos)
  - ✓ Por segmento físico
  - ✓ Por VLAN TAG 802.1Q,
  - ✓ Por rango de direcciones IP – CIDR
- ✓ La solución IDPS propuesta debe soportar la capacidad de bloquear ataques de reconocimiento.
- ✓ El IDPS debe contar con capacidades de Machine Learning que permita detectar brechas de seguridad que no pueden ser descubiertas por las soluciones de detección tradicionales basadas en firmas: contenido HTML malicioso incluyendo JavaScript, archivos maliciosos y objetos maliciosos de Adobe incluyendo Flash y PDF, permitiendo identificar todos estos en tiempo real
- ✓ La solución debe contar con la capacidad de monitoreo de tráfico encapsulado por lo menos de los siguientes tipos: VLANs, incluyendo frames 802.1q, GRE, Mobile IPv4 (IP-in-IP), IPv6 (6-in-4, 4-in-6, 6-in-6), Tuneles Authentication Header (AH), GPRS
- ✓ Realizar un monitoreo transparente para los usuarios donde de forma automática bloquee ataques maliciosos preservando la disponibilidad del ancho de banda de redInterfaz de monitoreo en modo pasivo como IDS sin afectar el tráfico
- ✓ La solución ofertada debe contar con una herramienta gráfica para la creación de firmas o filtros personalizados y se proporcionara sin costo para la institución.
- ✓ La solución IDPS propuesta debe permitir identificar y bloquear la comunicación con servidores, y deberá poder realizar la detección de amenazas avanzadas tales como Back Orifice, port scans, sensitive data, datos predefinidos y que aplique los controles directamente a la consola de administración de la solución para automatizar el proceso de detección y contención.
- ✓ La implementación de la solución IDPS propuesta por el proveedor no deberá requerir la modificación de routers o switches para su implementación, funcionado como puente en la red
- ✓ La solución IDPS debe proteger a los usuarios contra sitios de phishing, correos de spam y phishing, prevenir la descarga de trojanos, malware, spyware y gusanos
- ✓ La solución IDPS propuesta debe permitir alertar y bloquear comunicaciones desde y hacia determinados países
- ✓ La solución propuesta debe incluir filtros de protección para al menos los siguientes protocolos: CIFS, DNS, FTP, HTTP, ICMP, IMAP, KERBEROS, POP3, RDP, SIP, RTSP, SMTP y TFTP
- ✓ La solución propuesta debe incluir filtros de detección de las siguientes aplicaciones: Facebook, , LINKEDIN, SKYPE, TWITTER, YOUTUBE, Gmail, Yahoo Mail, Evernote, YousendIt, DropBox, 4Shared, Megaupload, iTunes, Netflix, Grokster, Jabber, Unreal Tournament, Second Life, Hamachi VPN, SoftEther VPN, Teamviewer, HotSport SHield, Kazaa, Gnutella, Morpheus, Gnucleus, iMesh, GotoMyPC, BitTorrent, Yahoo Messenger, Blubster, eDonkey, eMule, Twister, Ares, Jabber, SoftEther VPN, Megaipload, JXTA, yousendit
- ✓ La solución debe proveer protección como mínimo contra ataques de tipo SQL Injection, Command Injection, Cross Site Scripting, Buffer/Heap Overflow, DDoS
- ✓ La solución propuesta debe contar con integración con herramientas de escaneo de vulnerabilidades de aplicaciones que permita utilizar el reporte generado por la herramienta de escaneo para generar de forma automática una firma o filtro para protección contra las vulnerabilidades descubiertas por la herramienta de escaneo

- ✓ Debe permitir el reensamblado de paquetes y sesiones fragmentadas
- ✓ Debe resistir al menos las siguientes técnicas de evasión; las cuales se mencionan en forma enunciativa no limitatva:
  - o IP FRAGMENTATION
  - o TCP STREAM FRAGMENTATION
  - o RPC FRAGMENTATION
  - o URL OBFUSCATION

Se deberá incluir el acceso al portal de información de Investigación en Seguridad e Inteligencia de Amenaza Global del fabricante.

- ✓ El fabricante del IDPS propuesto, debe contar con un portal que podrá ser consultado, vía web, con las estadísticas en los últimos años con el número de vulnerabilidades de Zero Day descubiertas por su programa de investigación a través de un documento o una liga pública en internet.
- ✓ La solución IDPS propuesta debe contar con la actualización automática de filtros y firmas al menos conforme las libere el fabricante y durante los 3 años del soporte.
- ✓ La solución de IDPS propuesta debe proveer un portal de inteligencia global de amenazas que provea monitoreo en tiempo real y estadísticas de amenazas y ataques y pueda ser accesible desde la misma interfaz de la consola de monitoreo y control de la solución.
- ✓ El portal debe tener la capacidad de mostrar la actividad de los ataques basado en continentes y países.
- ✓ El portal debe permitir mostrar la fuente y destino de la amenaza en cada tipo de ataque.
- ✓ El portal debe tener la capacidad de monitorear y destacar las nuevas y crecientes amenazas.

Servicios de Reputación por IP

- ✓ La oferta deberá incluir un servicio de reputación de sitios a nivel de IP por los 3 años del contrato, que permita ejecutar controles sobre un sitio o Host en base a la lista de reputación del portal de servicios de reputación del mismo fabricante del equipo.
- ✓ El portal debe tener la capacidad de monitorear y destacar las nuevas y crecientes amenazas
- ✓ El IDPS propuesto debe ser capaz de bloquear tráfico basado en un servicio de reputación en la nube, la base de datos de reputación debe incluir direcciones IP y entradas de DNS de los sitios conocidos como peligrosos tanto para IPv4 como para IPv6
- ✓ El servicio de reputación debe incluir categorías de Malware, Botnet, Spyware, spam y Mobile, así como la capacidad de bloquear de forma selectiva
- ✓ Las definiciones de para la protección contra SPYWARE y VIRUS debe realizarse de forma automática, programada por fecha y hora como mínimo dos veces por mes durante la vigencia del contrato
- ✓ El IDPS debe soportar reputación basado tanto en dirección IP como en nombre del dominio.
- ✓ La base de datos de reputación debe ser alimentada con diferentes fuentes de reputación
- ✓ Las políticas de reputación deben tener la flexibilidad para ser aplicado en modo Permitir o Bloquear
- ✓ La política de reputación debe soportar filtrado basado en Geolocalización
- ✓ Deberá ser reconocido como líder dentro del Cuadrante Mágico de GARNER para el rubro de Detecntion and prevention Systems más recientemente publicado.

- ✓ Basado en marcos que permitan ampliar la protección con servicios de seguridad e integración de con soluciones de terceros, opción para soportar cuarentena de tráfico, riesgoso mediante la integración común dispositivo tipo FW para hacer un cambio de regla en este y contar con diversos paquetes de filtros para la protección y otros filtros personalizados de acuerdo a las necesidades del INAI.
- ✓ Deberá mostrar para cualquier evento el origen y el destino del ataque o incidente de seguridad
- ✓ Deberá soportar la descarga de paquetes, al generarse un evento de intrusión, para protecciones específicas con el fin de realizar análisis forenses.

Sistema de Administración

- ✓ Administración Local
  - ✓ El IDPS propuesto debe ser administrable desde un servidor de administración centralizado
  - ✓ El IDPS propuesto debe soportar SNMP para administración del dispositivo
  - ✓ El IDPS propuesto debe soportar la opción de enviar mensajes de syslog, SNMP traps y correos electrónicos
- ✓ Administración Centralizada
  - ✓ El IDPS propuesto debe soportar un servidor de administración centralizada para administrar todos los dispositivos IDPS.
  - ✓ El servidor de administración centralizada debe operar como una máquina virtual no un hardware dedicado y deberá ser implementado en infraestructura VMware propia del INAI.
  - ✓ El sistema de administración propuesto debe incluir la capacidad de administrar por lo menos 2 IDPS sin necesidad de licenciamiento adicional.
  - ✓ El sistema de administración propuesto debe permitir la descarga de las últimas firmas de manera manual y automáticamente
  - ✓ El sistema de administración propuesto debe permitir la distribución de las últimas firmas de manera manual, automática o permitir la calendarización para distribuir a varios dispositivos IDPS
  - ✓ El sistema de administración propuesto debe contar con un dashboard que permita mostrar las alertas de seguridad detectadas y la salud de los IDPS, este dashboard debe ser customizable
  - ✓ El servidor de administración debe contar con capacidad integrada de reporteo incluyendo reportes para Top N de ataques, origen de los ataques, destino de los ataques, top de aplicaciones, Top reputación por País
  - ✓ El servidor de administración centralizado debe soportar la generación de reportes manual o calendarizados diariamente, semanalmente, mensualmente, etc.
  - ✓ El servidor de administración centralizado debe permitir exportar el reporte al menos en los formatos PDF
  - ✓ El servidor de administración debe soportar archivar y hacer backup de eventos
  - ✓ El sistema de administración propuesto debe ser capaz de proveer diferentes niveles de cuentas de usuarios y acceso de administración con al menos 3 perfiles
  - ✓ La solución debe poder como opción el soportar integración con herramientas SIEM y enviar logs en formato CEF.
  - ✓ La solución de administración centralizada debe permitir la administración de los IDPS ofertados
  - ✓ La solución de administración centralizada debe permitir implementar acciones automáticas ante la detección de una alerta de seguridad como, por ejemplo:

redireccionar a un usuario a un portal de remediación, mover a un cliente a una VLAN segura o removerlo de la red

- ✓ La solución de administración centralizada debe soportar esquemas de Alta disponibilidad, es decir soportar la configuración de 2 consolas en un esquema de HA.
- ✓ La solución de administración centralizada debe permitir importar los resultados de soluciones de escaneo de vulnerabilidades
- ✓ La solución de administración centralizada deberá comparar los resultados de escaneo de vulnerabilidades importados y hacer recomendaciones de filtros o políticas a habilitar para mitigar las vulnerabilidades identificadas.

5.6. CAPA DE HARDWARE PARA LA DETECCIÓN Y PROTECCIÓN CONTRA AMENAZAS AVANZADAS

El licitante deberá proponer como alcance de su oferta, la infraestructura (hardware/software) necesaria para cubrir la funcionalidad de la capa de detección y protección de amenazas avanzadas

El licitante deberá proponer una solución de protección frente a amenazas avanzadas que proporcione visibilidad e inteligencia en toda la red, su despliegue deberá ser en modo de monitoreo, es decir fuera de línea, permitiendo la supervisión del tráfico de red, para no interrumpir la operación.

La solución deberá ser basada como mínimo en un equipo Hardware de propósito específico para realizar su función, ya que no se aceptarán soluciones basadas en hardware y software de propósito común.

De preferencia la solución propuesta deberá tener la capacidad de integrarse nativamente con la solución de sistema de prevención, detección y protección contra ataques mediante la misma consola del IDPS, de manera que le proporcione una visión global y control de políticas de seguridad para gran escala y contar como mínimo con las siguientes características y funcionalidades:

Hardware

- ✓ Los equipos ofertados deberán ser bajo una plataforma de hardware de propósito específico denominado "hardware" con software propiedad del mismo fabricante del Hardware, no se aceptarán soluciones de SW integradas en servidores de terceros.
- ✓ Throughput Nominal mínimo de 1 Gbps.
- ✓ Contar con Fuentes de poder redundantes AC, entradas de voltaje de 220 VAC que se puedan remover en caliente (hot-swap) con cable con conector nema C14.
- ✓ Dos discos duros con capacidad de 1 TB con sistema contra fallas, como por ejemplo el arreglo de discos RAID1.
- ✓ Al menos 2 puertos 10/100/1000 BateT
- ✓ Montable en rack de 19 pulgadas.

Colector

- ✓ No deberá ser disruptivo ante ningún servicio informático que la institución brinde, es decir; no deberá bloquear ningún tráfico, no deberá agregar latencia ni deberá operar "en línea", bajo ninguna circunstancia, sobre ningún paquete de red.
- ✓ La recepción y análisis del tráfico de red deberá ser posible única y exclusivamente mediante la lectura y recepción de puertos de monitoreo (port mirror o port span) que envíen la totalidad del tráfico de red a analizar.
- ✓ La recepción y análisis del tráfico de red deberá ser posible sin la necesidad de integración con ningún servicio o infraestructura de la institución, y sin la necesidad de instalar agentes de software en ningún dispositivo a monitorear.
- ✓ Deberá tener la capacidad de detectar y analizar, dentro del tráfico entregado por la institución:
    - o Amenazas y riesgos de cualquier dispositivo IP independientemente de su plataforma o sistema operativo, que se conecte a la red monitoreada, y que atente contra la integridad, disponibilidad y confidencialidad del flujo y contenido de la información.
    - o Ataques dirigidos con el objetivo de extraer, robar u obtener por medios digitales información.
- ✓ Deberá brindar todos los elementos de inteligencia de amenazas necesarios para poder determinar el origen, las acciones y el impacto de la misma con el objetivo de implementar recomendaciones en la infraestructura analizada para poder responder al ataque antes de que cause un daño significativo.
- ✓ Deberá descubrir el comportamiento malicioso de dispositivos que no cumplen con los requerimientos mínimos de seguridad institucionales.
- ✓ Deberá poder identificar amenazas que son evasivas a la seguridad tradicional de firewalls, detectores de intrusos y antivirus.
- ✓ Deberá poder brindar un análisis forense de las amenazas en un ambiente de simulación (sandbox) local.
- ✓ El ambiente de simulación deberá soportar sistemas operativos simulados de la plataforma Windows 7, 8.x, 10, server 2003 y 2008, en sus versiones de 32 y 64 bits
- ✓ Deberá proveer un reporte detallado en formato PDF y en HTML, sobre el comportamiento de la amenaza detectada en el o los ambientes de simulación, indicando la conducta y los cambios detectados en cada uno de los ambientes simulados.
- ✓ Deberá proveer la muestra de la amenaza, junto con la captura de paquetes del tráfico generado durante su ejecución en el ambiente simulado, en el caso que así aplique.
- ✓ Deberá poder identificar amenazas utilizando inteligencia global, inteligencia local, inteligencia personalizada y correlación entre las mismas.
- ✓ Deberá correlacionar información de protocolos y sesiones en todo el volumen del tráfico analizado, identificando posibles riesgos y amenazas de seguridad.
- ✓ Deberá detectar y correlacionar comportamientos del atacante en la red interna como, por ejemplo:
    - o Movimiento lateral

- Accesos y consultas a bases de datos
- Transferencia de archivos
- Accesos a escritorios remotos

✓ Deberá poder obtener el usuario de directorio activo involucrado en el incidente aun cuando el dominio no sea el institucional sin la necesidad de integración directa con el directorio activo de la institución.

✓ Deberá poder analizar no sólo archivos ejecutables, sino también archivos de documentos que puedan ser utilizados para explotar vulnerabilidades en aplicaciones independientes al sistema operativo.

✓ Deberá ser capaz de detectar servicios DNS, DHCP y SMTP no declarados a la institución.

✓ Deberá ser capaz de detectar aplicaciones móviles maliciosas.

✓ Deberá ser capaz de detectar dispositivos móviles accediendo a servidores críticos, a través de conexiones remotas.

✓ Deberá ser capaz de identificar y analizar amenazas transmitidas en al menos 100 protocolos de red, en cualquier puerto, tanto tráfico entrante como saliente, incluyendo HTTP, SMTP, POP3, FTP, DNS, IRC, SMB, RDP, SQL, IMAP4 y Bittorent, entre otros.

✓ Deberá brindar la información disponible, en todo momento, de los incidentes de seguridad detectados a través de un tablero de resultados (dashboard).

✓ Deberá poder detectar mecanismos de ocultamiento y evasión de análisis de tráfico, redes TOR, UltraSurf, características de tráfico SSL malicioso, entre otras.

✓ El componente habilitador deberá poder notificar de sus hallazgos utilizando los siguientes formatos Syslog, SNMP o correo electrónico.

✓ De ser requerido, el componente habilitador podrá instalarse dentro de un ambiente virtual VMWare para analizar tráfico dentro de la infraestructura virtual de la institución utilizando el virtual Switch.

✓ Deberá tener la capacidad de configurar inteligencia local personalizada que permita la detección de los siguientes componentes:

- Archivos mediante SHA-1 ingresado manualmente o mediante la subida de un archivo
- Direcciones IP
- URL
- Dominios

✓ El componente habilitador deberá realizar capturas de la red a través de PCAP, permitiendo buscar indicios y conexiones durante y en todo el momento de un incidente.

✓ El componente habilitador deberá ser capaz de alinear los eventos de seguridad a las diferentes etapas del modelo cadena de progresión de la amenaza.

✓ El componente habilitador deberá ser capaz de importar reglas personalizadas YARA para profundizar en el análisis realizado durante la inspección de tráfico.

✓ El sandbox deberá tener la capacidad de utilizar técnicas de Machine Learning dentro de sus motores para la detección de amenazas en los archivos analizados.

Analizador

- ✓ Deberá poder analizar y diagnosticar de manera automática, archivos adjuntos, y documentos PDF, Word, Excel, ZIP, Flash, scripts.
- ✓ Podra tener integración nativa con las soluciones de seguridad como el firewall o IDPS, de tal manera que pueda enviar los indicadores de compromiso analizados de alto riesgo, de forma inmediata
- ✓ De acuerdo al resultado del análisis realizado deberá retroalimentar de forma automática a las soluciones correspondientes para que ejecuten las acciones de contención.
- ✓ Deberá poder brindar un análisis forense de las amenazas en un ambiente de simulación (sandbox) local, automatizado, personalizado y aislado.
- ✓ El ambiente de simulación deberá soportar sistemas operativos simulados de la plataforma Windows 7, 8.x , 10, Windows server 2003 y 2008, en sus versiones de 32 y 64 bits
- ✓ De ser requerido el componente habilitador contará con al menos 6 ambientes de simulación simultáneos dentro del mismo componente, pudiendo ser estos una combinación de ambientes personalizados y/o ambientes por defecto.
- ✓ Deberá proveer un reporte detallado en formato PDF o HTML, sobre el comportamiento de la amenaza detectada en el o los ambientes de simulación, indicando la conducta y los cambios detectados en cada uno de los ambientes simulados,
- ✓ Deberá proveer la muestra de la amenaza, junto con la captura de paquetes del tráfico generado durante su ejecución en el ambiente simulado, en el caso que así aplique.

5.7. SERVICIO DE PROTECCIÓN AVANZADA PARA SERVIDORES

Dados los diferentes vectores de nuevos ataques que van apareciendo en los últimos años el INAI requiere contar con una estrategia de defensa a nivel más granular y que a su vez permita contar con la visibilidad necesaria sobre los elementos que corren en 10 servidores críticos de la institución.

La solución deberá así mismo operar de forma integrada con los sistemas de protección de perímetro y zonas, así como los de visibilidad de red requeridos en esta licitación.

Con la solución propuesta se deberá poder llevar los controles de FW, IPS, y antimalware a nivel de Host para completar la estrategia total de seguridad en todas las capas.

La solución propuesta tendrá que operar de manera sincronizada con las otras capas integradas por la consola de gestión centralizada antes mencionada.

Sistemas operativos

Deberá cubrir como mínimo los siguientes sistemas operativos:

- Windows Server 2000
- Windows Server 2003 SP1, SP2 y R2 SP2 (32/64 bit).

- Windows Server 2008 (Full) (32/64 bit)
- Windows Server 2008 R2 (Full) (64 bit)
- Windows Server 2012 (Full) (64 bit)
- Windows Server (Full or Core) 2012 R2 (64-bit)
- Windows Server 2016 Version 1607 (64-bit)
- Windows Server 2016 Version 1709 (RS3) (64-bit)
- Windows Server 2016 Version 1803 (RS4) (64-bit)

o Solaris™:
- Solaris 10 Update 4-11 (64-bits, SPARC o x86)
- Solaris 11.2, 11.3 (64-bit, SPARC o x86).

o Linux:
- Red Hat® Enterprise 5, 6, 7 (32/64 bit)
- SUSE® Enterprise 10 SP3, SP4
- SUSE® Enterprise 11 SP1, SP2, SP3 (32/64 bit)
- SUSE® Enterprise 11 SP4 (64 bit)
- CentOs 5 y 6 (32/64 bit)
- CentOs 7 (64 bit)
- Oracle Linux 5 y 6 (32/64bit)
- Oracle Linux 7 (64 bit)
- Ubuntu 10.04, 12.04, 14.04, 16.04, 18.04, LTS (64-bit)

Firewall

- El servicio de administración deberá contener un firewall que proteja servidores físicos y virtuales administrados desde la misma consola, permitiendo sólo las comunicaciones requeridas entre ellos. Este filtrado debe ser bidireccional y hacerse al menos sobre los siguientes parámetros:
  - Protocolos: ICMP, IGMP, TCP, UDP, TCP+UDP
  - Direcciones MAC
  - Direcciones IP
  - Puertos TCP & UDP
  - Plantillas con reglas predefinidas para plataformas comunes

IPS de Host

- El servicio deberá ser capaz de realizar una inspección bidireccional profunda de los paquetes para analizar y prevenir ataques a vulnerabilidades en las aplicaciones instaladas en cada servidor, incluidas vulnerabilidades de día cero.
- El proveedor del servicio deberá monitorear el tráfico para registrar algún ataque, y además tener la capacidad de realizar acciones de bloqueo.
- El proveedor del servicio deberá monitorear el tráfico para registrar algún ataque y bloquear el tráfico relacionado con él sin afectar el tráfico normal no relacionado con el ataque, permitiendo que continúen disponibles los servicios del servidor.

Antimalware en el Servidor

- El servicio deberá garantizar:

- Que el módulo de antivirus debe ser especializado para integrarse con VMWare vSphere y ser capaz de brindar la protección sin necesidad de instalar un agente para plataformas Windows y Linux.
- Garantizar la exploración en tiempo real, programada y manual de todos los archivos en servidores virtuales con sistema operativo Windows Server 2012 (64-bit), Windows Server 2008 (32-bit and 64-bit), Windows Server 2008 R2 (64-bit), Windows Server 2003 R2 (32-bit and 64-bit), Windows Server 2003 SP2 (32-bit and 64-bit).

- Los escaneos en tiempo real, los escaneos programados y los escaneos bajo demanda deben contar con la posibilidad de manejar excepciones en función de: tipos de archivos y rutas.
- Los escaneos deben de contar con caché para los escaneos en tiempo real y programados, con el objetivo de optimizar el consumo de recursos en los servidores virtuales.

Amenazas de Día Zero

- Se tiene la capacidad de enviar muestras de archivos sospechosos para detectar amenazas de día cero, a través de la integración de preferencia nativa y automática con el Componente Habilitador de Retroalimentación y Respuesta Automática contemplado en el Servicio de Detección y Protección contra Amenazas Avanzadas.
- La solución deberá de ser capaz de consumir y desplegar los indicadores de compromiso identificados por el Componente Habilitador de Retroalimentación y Respuesta Automática, hacia todos los agentes en los puestos de servicio, permitiendo tomar una acción para futuras detecciones.

Reputación Web

- El servicio deberá de incluir en la integración con los servicios de reputación (del mismo fabricante) para mejorar la protección contra amenazas, incluyendo servicio de reputación de archivo y reputación de URL's.
- El servicio deberá de contemplar la funcionalidad de reputación de URL's debe evitar la conexión a sitios de mala reputación que puedan poner en riesgo la información que reside en los servidores de INAI.
- El servicio deberá de tener la funcionalidad de reputación de URL's debe permitir el manejo de excepciones y configurarse mediante umbrales.

Monitoreo de cambios de archivos y carpetas criticas (Integrity Monitoring)

- El proveedor del servicio deberá identificar los cambios en archivos críticos, cambios a la configuración de archivos, carpetas, servicios y llaves de registro tanto del sistema operativo como de las aplicaciones instaladas en el servidor. Bajo las plataformas de Windows y Linux soportadas es necesario la identificación en tiempo real.
- El proveedor del servicio debe ser capaz de identificar y aplicar automáticamente reglas de monitoreo sobre cambios realizados en archivos, carpetas y llaves de registro críticas del sistema operativo y las aplicaciones instaladas en el servidor.

Control de Aplicaciones

El servicio deberá de garantizar:

- Debe de ser capaz de una vez habilitado el componente, realizar un escaneo que permita buscar el inventario de programas instalados para crear un conjunto de reglas locales, permitiendo la ejecución de los programas identificados.
- Debe de monitorear de forma continua con el fin de detectar cualquier cambio tanto a nivel del kernel y archivos de sistema realizados por los programas al momento de la instalación o nuevas ejecuciones.
- Debe de registrar todos los cambios de software. Los eventos se generan cuando el control de aplicaciones detecta software nuevo o modificado en el sistema de archivos, y cada vez que el software intenta ejecutarse.

Monitoreo de bitácoras del sistema operativo y aplicaciones

- La solución debe inspeccionar bitácoras de sistema operativo y aplicaciones para identificar eventos de seguridad que se consideren relevantes o críticos.
- Las alertas podrán ser enviadas por correo electrónico o por syslog con el fin de poder ser explotadas.
- Capacidad de crear reglas personalizadas para el monitoreo de bitácoras.
- Capacidad de inspeccionar eventos generados por aplicaciones los cuales sean almacenados en archivos de bitácoras.
- La solución debe tener la capacidad de inspeccionar eventos generados:
  - En el visor de eventos para los servidores de plataformas Windows.
  - En el syslog messages de servidores con sistema operativo Linux.

REST API

La solución deberá tener documentado un API que permita automatizar tareas administrativas, incluyendo funcionalidades de autenticación, administración cuentas de nube, eventos, monitoreo, escaneos de imágenes de contendores.

6. SERVICIOS DE IMPLEMENTACION, INTEGRACIÓN DE LA INFRAESTRUCTURA Y SOPORTE TÉCNICO.

El licitante como parte de su propuesta deberá considerar servicios profesionales de implementación de todos los componentes de la infraestructura (hardware y software) propuestos desde su configuración, pasando por la puesta a punto y puesta en producción, los cuales serán validados por el personal de la DGTI del INAI designado.

Los servicios profesionales de implementación deberán estar cubiertos con especialistas directamente en sitio en las instalaciones del INAI durante toda la fase de implementación y deberán contar con experiencia en las plataformas a implementar de la siguiente manera:

- Por lo menos 5 recursos certificados (uno por cada capa de seguridad) cubriendo como mínimo una certificación por cada una de las soluciones ofertadas en cada una de las marcas utilizadas en las soluciones ofertadas para cubrir los requerimientos que garantice que el Licitante puede ofertar soporte de la plataforma ofertada, un recurso del licitante puede cubrir hasta dos certificaciones distintas.

- 2 recursos certificados en VMWare para el apoyo en la implementación de las plataformas que puedan ser montadas en los ambientes virtualizados del INAI

La experiencia de cada recurso será comprobada a través de la validación del curriculum vitae y con la copia simple del certificado correspondiente, dichos documentos serán validados por el administrador del contrato designado por la DGTI

En caso de suscitarse un cambio en el personal asignado por causas de fuerza mayor, el proveedor deberá cubrir al personal con las mismas características descritas con anterioridad y este deberá presentar su curriculum vitae y certificaciones correspondientes, dichos documentos serán validados por el administrador del contrato designado por la DGTI.

Los recursos certificados en las soluciones ofertadas asignados, deberán contar con experiencia comprobable para la atención de incidentes o problemas sobre las soluciones implementadas para cubrir las diferentes necesidades de la organización, así mismo como requerimientos específicos (cambios de configuraciones, actualizaciones, alta de nuevas funcionalidades) realizados sobre la infraestructura propuesta, la cual será validada a través de la presentación curriculum vitae, y de las constancias de cursos y/o certificaciones en las marcas utilizadas en las soluciones ofertadas para cubrir los requerimientos de este Anexo Técnico.

Así mismo, se deberá considerar la migración de la configuración de la infraestructura existente actualmente hacia la nueva solución propuesta, conservando todas las políticas actuales de FW y los filtros de IDPS y cargando estas hacia la nueva plataforma NGFW y IDPS, haciendo finalmente la verificación de su correcta funcionalidad, en el entorno del INAI.

El licitante deberá demostrar mediante contratos que ha llevado a cabo una migración similar en cuando menos tres de las plataformas ofertadas dentro de los últimos 4 años anteriores.

Posteriormente durante el contrato el Licitante irá depurando las políticas, así como los filtros y firmas con base a un plan de trabajo pactado de común acuerdo con el administrador del contrato designado por la DGTI del INAI, mediante ventanas de autorización bajo un estricto control de cambios con apego total a las mejores prácticas de ITIL, lo cual deberá estar controlado por el administrador de proyecto por parte del proveedor y el cual deberá firmar todas las minutas de control de cambios durante el contrato.

Como parte de la propuesta técnica, el Licitante deberá presentar:

6.1. PLAN DE TRABAJO DETALLADO

Plan de trabajo que incluya las actividades necesarias, a fin de cubrir la implementación, y entregables requeridos por el Instituto en el presente documento para cada una de las soluciones, las características del plan de trabajo se detallan a continuación:

Como parte del alcance de su propuesta técnica, el Licitante deberá entregar el plan detallado de trabajo, que permita conocer a la DGTI las actividades y tiempos estimados que este requerirá para la implementación de la solución integral que oferte.

El plan de trabajo propuesto por el Licitante deberá cumplir de forma mínima, con las actividades establecidas en el Plan de Trabajo General, que se detalla más adelante, el cual será el punto de partida para que el Licitante elabore su Plan de Trabajo Detallado obligatorio. Si bien los tiempos y actividades serán propuestos por cada licitante, deben

tomar como base el plan de trabajo general y no deberán exceder las fechas establecidas en el presente anexo.

El proveedor deberá agregar las fases y tareas necesarios, y tiempos específicos para adecuar el plan de trabajo detallado entregado en su propuesta, y generar un plan de trabajo final, que será entregado a más tardar 10 días hábiles posteriores a la notificación del fallo.

6.2. PLAN DE TRABAJO GENERAL

Etapa del Proyecto	Tarea	Sem 1	Sem 2	Sem 3	Sem 4
1) Planeación	**Formalizar Plan de Trabajo**				
2) Implementación	**Recepción de Equipos**				
	Instalación de Equipos				
	Puesta a punto de infraestructura				
3) Transición	**Transferencia del Conocimiento**				
	Migración del Servicio				
4) Producción	**Salida a Producción**				
5) Soporte y Acompañamiento	**Soporte en Sitio**				
	Soporte a través de Mesa de ayuda				

6.3. SOPORTE TÉCNICO

Los equipos deberán ser entregados con garantía del fabricante por la vigencia del contrato en todos los componentes propuestos tanto en hardware como en software. También se deberá considerar el nivel de servicio como sigue:

- La respuesta para la atención de incidentes en los equipos de seguridad, deberá ser no mayor a dos 2 horas naturales. En caso de que se requiera atención en sitio, la solución deberá ser no mayor a seis 6 horas naturales.

En cuanto a la revisión y aplicación de actualizaciones de software, ésta se deberá realizar de manera anual de acuerdo a la vigencia de la garantía del microcódigo y parches a los equipos y software siempre y cuando la capacidad del hardware instalado lo permita, esta actividad estará a cargo del proveedor mediante autorización del administrador del contrato de la DGTI.

El proveedor deberá especificar por escrito el procedimiento para la atención a incidentes, los tiempos de respuesta y la matriz de escalamiento mediante una mesa de ayuda.

6.3.1. MESA DE AYUDA

6.3.1.1. MODO DE OPERACIÓN DE LA MESA DE AYUDA

Para la prestación del presente servicio el licitante deberá de contar con una mesa de ayuda alineada a los procesos de ITIL, la cual será proporcionada sin costo para el Instituto con la finalidad de generar los reportes y la canalización de Incidencias por parte del personal autorizado de la DGTI sin importar su nivel de atención hacia la mesa de Ayuda del Licitante. Siendo alcance del Licitante la atención, seguimiento y remediación de incidentes de falla asociados a los bienes y servicios solicitados en este Anexo Técnico.

El servicio de la mesa de ayuda estará compuesto como mínimo de 5 operadores de mesa con experiencia de cuando menos un año en atención a requerimientos a través de una mesa de ayuda y con acreditación de cursos de administración u operación de la mesa propuesta para el cumplimiento de este Anexo Técnico, dicha experiencia será comprobada a través de la validación del curriculum vitae de cada operador y la acreditación correspondiente descrita con anterioridad, mismas que serán validadas por el administrador del contrato designado por la DGTI.

En caso de suscitarse un cambio en el personal asignado como operadores de mesa, el proveedor deberá cubrir al personal con las mismas características descritas con anterioridad y este deberá presentar su curriculum vitae y acreditaciones correspondientes de cursos de administración u operación de la mesa propuesta, dichos documentos serán validados por el administrador del contrato designado por la DGTI.

Primer Nivel: Mesa de Ayuda.
El primer nivel de atención realizará entre otras las siguientes actividades:

1. La recepción centralizada de reportes de incidentes, problemas y requerimientos por parte de los usuarios autorizados de la DGTI.
2. El registro de incidencias, problemas y/o requerimientos se hará a través de la herramienta tecnológica de la Mesa de Ayuda del Proveedor, generando un identificador/folio denominado ticket el cual será canalizado para su atención y solución de acuerdo con los niveles de servicio acordados en este Anexo Técnico.
3. La elaboración de un diagnóstico definitivo o preliminar para aquellos servicios que no puedan ser provistos en modo de autoservicio.
4. La solución o el escalamiento al Segundo nivel de atención para Soporte Especializado.
5. El primer nivel de atención de la Mesa de Ayuda será el único responsable de mantener actualizado y en permanente monitoreo el estado de los tickets escalados para informar a la DGTI, el estatus de los mismos.
6. El cierre centralizado de los tickets registrados previa confirmación de la solución, mediante la aprobación del personal autorizado de la DGTI.
7. La documentación e integración de las soluciones a los tickets registrados, en la base de datos de conocimientos, debidamente clasificados y agrupados para su eficiente consulta.
8. Realizar sesiones de retroalimentación a su personal en las que se revisen los incidentes frecuentes y las soluciones existentes en la base de datos de conocimiento para asegurar su correcta utilización y llevar a cabo la mejora continua de los procesos.
9. Realizar la medición, monitoreo y revisión de las estadísticas operativas, de calidad del servicio de la Mesa de Ayuda a los incidentes de manera trimestral.
10. Cumplir los niveles de servicio pactados para cada categoría y/o servicios.

6.3.1.2. CARACTERÍSTICAS MÍNIMAS DE LA MESA DE AYUDA

Herramienta Operativa

El Proveedor deberá aprovisionar una herramienta para la gestión de la mesa de ayuda la cual deberá estar operando al día siguiente del fallo, con las siguientes características:

A. La herramienta deberá estar alineada a cuando menos 11 procesos ITIL:
    1. Gestión de Cambios (CHG)
    2. Gestión de Eventos (EV)
    3. Gestión de Incidentes (IM)

4. Gestión del Conocimiento (KM)
5. Gestión de Problemas (PM)
6. Gestión de la Entrega y Despliegue (REL)
7. Gestión de Solicitudes (RF)
8. Gestión de Activos de Servicio y de la Configuración (SACM)
9. Gestión del Catálogo de Servicios (SCM)
10. Gestión de Niveles de Servicio (SLM).
11. Gestión del Portafolio de Servicios (SPM)

Para lo cual deberá presentar en su propuesta el nombre comercial de la herramienta de mesa de ayuda a utilizar y presentará dentro de su propuesta evidencia documental, URL, hojas de datos técnicos del fabricante y una carta firmada por el representante legal del licitante en la que se indique que cuenta con la mesa de ayuda en comento.

B. Para la gestión de incidentes y solicitudes, la herramienta deberá permitir:
    1. Gestionar el ciclo de vida de todo incidente o solicitud reportada
    2. Asignar un número de caso a las solicitudes o incidentes reportados para su identificación y seguimiento
    3. Administrar el estado de las solicitudes o incidentes durante su ciclo de vida. Por lo que debe contemplar por lo menos los estados: Abierto, Asignado, En espera y Cerrado, dichos estados son enunciativos más no limitativos, por lo que la DGTI podrá solicitar durante la vida del contrato añadir más estados, sin que esto requiera el uso de código o programación
    4. Clasificar los incidentes y solicitudes en categorías y subcategorías
    5. Configurar los servicios, categorías y subcategorías en que se clasificarán los incidentes y solicitudes, así como las prioridades y SLA's sin el uso de lenguaje de programación
    6. Generar reportes y estadísticas personalizados desde el portal web
    7. Deberá contar también con tableros de control y estadísticas que permitan identificar el estado en que se encuentren las solicitudes de servicio, El cual puede ser consultado por la DGTI mediante un portal web, sin que esto genere el uso de licenciamiento de la herramienta
C. Podrá generar flujos de trabajo o tareas automatizadas a través de una interfaz gráfica, sin necesidad del uso de lenguaje de programación
D. Permitirá también la administración de los Items de configuración (CI's) mediante una CMDB la cual es parte del sistema. Los CI's que sean reportados con falla a la mesa de ayuda, pueden ser asociarse al o los tickets que se generados, con el fin de identificar tendencias o elaborar estadísticas de falla.
E. Los reportes de incidentes que se generen deberán ser capaces de mostrar campos de los CI's alojados en la CMDB
F. En caso de requerirse modificaciones a los formularios de registro de incidentes o solicitudes, añadir nuevos estados o categorías, así como la creación o modificación de reportes, estas podrán ser realizadas sin el uso de lenguaje de programación o manipulación de código fuente y en un lapso de no mayor a 12 horas
G. La herramienta deberá tener la capacidad de realizar en tiempo real y de manera automática o manual, un respaldo de su información para asegurar la continuidad del servicio

6.3.1.3. REPORTES MENSUALES DE INCIDENTES

El proveedor deberá entregar durante los primeros 10 días hábiles posteriores a la finalización del mes, un reporte con los incidentes reportados a la Mesa de Ayuda, el cual incluirá la siguiente información:

- ✓ Tipo de solicitud
- ✓ Descripción de la falla o requerimiento
- ✓ Estado
- ✓ Nombre del solicitante
- ✓ Fecha y hora en que se realizó la solicitud
- ✓ Fecha y hora en que se dio solución
- ✓ Descripción de la solución

Este reporte incluirá un resumen ejecutivo donde se muestra la cantidad de reportes generados durante cada mes del trimestre en cuestión, así como el estado en que se encuentran.

6.3.1.4. REPORTES DE LA MESA DE AYUDA.

Durante las reuniones que la DGTI y el proveedor llevarán a cabo una vez adjudicada la licitación para definir y acotar los procesos, procedimientos y categorización de incidentes y solicitudes para el escalamiento y atención de incidentes y/o solicitudes relativos a los servicios definidos en la presente propuesta.

El proveedor contemplará como entregables los siguientes documentos:

- ✓ Propuesta en operación del servicio de mesa de ayuda.
- ✓ Procedimiento de atención a fallas, el cual deberá contener los medios de contacto
- ✓ Proceso para solicitar soporte
- ✓ Directorio de escalamiento con al menos tres niveles el cual deberá contener la siguiente información:
  - ✓ Puesto
  - ✓ Nombre del contacto
  - ✓ Teléfono de oficina y celular
  - ✓ Correo electrónico

6.4. MEMORIAS TÉCNICAS:

El Proveedor deberá entregar la Memoria Técnica para cada una de las soluciones implementadas. Las mismas deberán cubrir al menos:

- ✓ Solución implementada
- ✓ Descripción de las especificaciones técnicas
- ✓ Descripción del producto a nivel funcional
- ✓ Detalles de la configuración implementada de la correspondiente solución
- ✓ Claves de acceso al día de la entrega de la administración de los equipos y Consideraciones especiales que deberá tener el INAI.
- ✓ Diagrama de arquitectura de la solución final implementada
- ✓ Procedimientos básicos de operación y ligas de acceso a los servicios solicitados con una copia de la pantalla que muestre el acceso valido al servicio.
- ✓ Datos de acceso a la mesa de servicio del licitante, así como listado de equipos con número de serie y esquema de escalación conforme a los niveles de servicio requeridos en este anexo técnico.

- ✓ La memoria Técnica se deberá revisar por lo menos una vez al año y hacer los cambios necesarios cada vez que existan cambios mayores a la infraestructura como son reingenierías o cambios de nivel de firmware.

6.5. PRUEBAS Y ENTREGA

Al inicio del contrato en los primeros 10 días posteriores a la firma del contrato, se establecerá con el administrador del contrato de la DGTI el protocolo de pruebas de aceptación conforme a las especificaciones mínimas requeridas y que pueda corroborar la operación de los servicios tal cual son solicitados en estas bases.

Una vez que se haya realizado la migración de los servicios desde la infraestructura actual hacia la nueva infraestructura, el proveedor deberá presentar la documentación (actas de protocolo de pruebas aprobadas) como evidencia de la implementación del servicio.

Las pruebas a realizar en las dos fases antes descritas serán pactadas de común acuerdo entre el administrador del contrato por parte de la DGTI y el administrador del servicio de parte del Proveedor.

El licitante deberá demostrar mediante contratos que ha llevado a cabo una migración similar en cuando menos tres de las plataformas ofertadas dentro de los últimos 4 años anteriores.

6.6. TRANSFERENCIA DE CONOCIMIENTO

Con objeto de operar y mantener la infraestructura alcance de este Anexo Técnico, la DGTI requiere de la provisión de capacitación al personal que este designe, por lo que el licitante deberá presentar como parte de su oferta:

- ✓ Plan de transferencia de conocimientos para al menos tres personas, contemplando como alcance todos los componentes de las soluciones implementadas.
- ✓ La capacitación se acordará de forma conjunta con el administrador del contrato por parte de la DGTI y el administrador de proyecto por parte del proveedor.
- ✓ Deberá realizarse dentro de los primeros 30 días naturales posteriores a la notificación del fallo.
- ✓ Estas sesiones de transferencia de conocimientos deberán ser proporcionados por personal certificado en los productos por el fabricante y pueden ser integrantes del proveedor.
- ✓ Deberán ser impartidas en idioma español, en instalaciones del INAI, proporcionando material de consulta para el personal capacitado.
- ✓ Deberá entregar evidencia de la impartición de la capacitación y de la entrega de los materiales.

6.7. SERVICIOS ESPECIALIZADOS DE SOPORTE TÉCNICO Y ADMINISTRACIÓN BAJO DEMANDA

El servicio especializado de soporte técnico y la administración bajo demanda, deberán estar cubiertos con especialistas con experiencia en las plataformas a implementar de la siguiente manera

- Por lo menos 5 recursos certificados (uno por cada capa de seguridad) cubriendo como mínimo una certificación por cada una de las marcas de las soluciones ofertadas en cada una de las marcas utilizadas en las soluciones ofertadas para cubrir los requerimientos que garantice que el Licitante puede ofertar soporte de la

plataforma ofertada, un recurso del licitante puede cubrir hasta dos certificaciones distintas.

- 2 recursos certificados en VMware para la operación y soporte de las plataformas que deberá montar en los ambientes virtualizados del INAI.
- 3 recursos altamente especializados en Seguridad Informática, de los cuales cuando menos uno deberá tener posgrado (maestría) y los otros dos podrán tener un diplomado en Seguridad de la Información o certificación ISO 27001 o certificación CISM (Certified information security manager) o CISA (Certified Information Systems Auditor).

La experiencia de cada recurso será comprobada a través de la validación del curriculum vitae y con la copia simple del certificado correspondiente, dichos documentos serán validados por el administrador del contrato designado por la DGTI

Los ingenieros asignados deberán contar con experiencia comprobable para la atención de incidentes o problemas sobre las soluciones implementadas para cubrir las diferentes necesidades de la organización, así mismo como requerimientos específicos (cambios de configuraciones, actualizaciones, alta de nuevas funcionalidades) realizados sobre la infraestructura propuesta, la cual será validada a través de la presentación de las constancias de certificaciones en las marcas utilizadas en las soluciones ofertadas para cubrir los requerimientos de este Anexo Técnico.

En caso de suscitarse un cambio en el personal asignado, el proveedor deberá cubrir al personal con las mismas características descritas con anterioridad y este deberá presentar su curriculum vitae y certificaciones correspondientes, dichos documentos serán validados por el administrador del contrato designado por la DGTI

En cualquier caso, el servicio deberá ser brindado ante una solicitud o notificación por parte de personal de la DGTI al proveedor con por lo menos 1 día hábiles de antelación.

El servicio solicitado no comprende la administración u operación diaria de la infraestructura tecnológica, siendo esta responsabilidad de la DGTI, para lo cual se deberán hacer las transferencias de conocimiento sobre las plataformas ofertadas por el Ingeniero certificado de parte del fabricante, pero si cubrirá el soporte sin costo en las instalaciones del INAI mediante los recursos antes mencionados, en caso de suscitarse una falla en cualquiera de los componentes de las soluciones ofertadas para cubrir los requerimientos de este anexo técnico y siempre apegándose a los SLA´s descritos en este documento, posterior al registro de solicitud en la mesa de servicio del proveedor.

Como parte de la propuesta técnica, el licitante deberá presentar:

- ✓ Respuesta de nivel de cumplimiento de cada uno de los requerimientos solicitados para el servicio especializado de Soporte Técnico.
- ✓ Descripción del servicio especializado de Soporte Técnico propuesto con las consideraciones del mismo.
- ✓ Niveles de Servicio y métricas consideradas en el servicio especializado de Soporte Técnico propuesto.

6.8. REQUERIMIENTOS ESPECÍFICOS DEL SERVICIO

El INAI requiere el arrendamiento sin opción a compra de una solución de seguridad perimetral mediante un proveedor con experiencia comprobable de cuando menos 4 años en la implantación de sistemas de seguridad perimetral de la información, para lo cual

deberá presentar contratos que incluyan las plataformas ofertadas y contratos de servicios con por lo menos 3 de las plataformas ofertadas.

A continuación, se describen las características mínimas del servicio a ofertar, así como las actividades y niveles de servicio requeridos para los servicios especializados de soporte y los entregables mínimos correspondientes de cada una de las etapas del proyecto.

El servicio deberá incluir el acceso a un sistema de monitoreo global del fabricante que indique en tiempo real las amenazas que se están produciendo en todo el mundo, cuáles son las 10 principales amenazas con sus direcciones de origen y el tipo de amenazas, así como los filtros o políticas que permitirán a la DGTI mantener la salud de sus plataformas, en el mismo portal se deberá poder verificar los sitios de reputación cuestionable para que se pueda utilizar de manera automática la información y ser contenida por el sistema perimetral de seguridad.

6.9. ADMINISTRADOR DE PROYECTO PARA LA IMPLEMENTACIÓN DE LA SOLUCIÓN OFERTADA

El Proveedor deberá designar desde la formalización del contrato y hasta la puesta en producción de la solución ofertada a un Administrador de Proyecto (PM por sus siglas en Ingles), el cual deberá contar mínimo con estudios de nivel licenciatura (comprobable con título profesional y/o cédula), Certificación PM emitida por el PMI y certificado en ITIL v3, el cual presentará su curriculum vitae y certificaciones vigentes al administrador del contrato designado la DGTI.

Con objeto de garantizar la correcta ejecución de los trabajos de suministro, instalación, y puesta en punto de los equipos ofertados en la presente propuesta, el Licitante proveerá el servicio de un PM, quien será el punto de contacto entre el personal designado la DGTI y el Proveedor durante los trabajos de implementación de la solución ofertada en la presente propuesta.

El Administrador de Proyecto estará facultado por parte del proveedor para tomar decisiones en todo lo relativo al cumplimiento de la implementación de la solución con todos los bienes y servicios solicitados en este Anexo Técnico, además conocerá el alcance de los servicios, así como las normas y especificaciones aplicables a éstos.

Lo anterior proporcionará la certeza de contar con un profesional que identificará las fortalezas, oportunidades, debilidades y amenazas de la fase de implementación del proyecto, ayudando a eliminar los obstáculos que pudieran evitar el éxito del plan inicial a través de la ejecución y gestión eficaz de las siguientes actividades:

- ✓ Administración del proyecto, desde la planeación, asignación de roles y responsabilidades de los recursos involucrados
- ✓ Planificación y programación de las actividades del Proyecto
- ✓ Control y seguimiento de actividades
- ✓ Facilitar el entendimiento y la comprensión de los objetivos del proyecto
- ✓ Incrementa la coordinación y cooperación entre el equipo de trabajo asignado al proyecto
- ✓ Seguimiento y aseguramiento al cumplimiento de objetivos y entregables del proyecto de acuerdo al plan de trabajo y con la calidad acordada en contrato.
- ✓ Seguimiento a control de cambios y solicitudes por parte de la DGTI
- ✓ Ejecución del proceso de entrega (Implementación a la Operación de los bienes y servicios ofertados en la presente propuesta)

Este servicio de PM será provisto de manera continua por una sola persona desde la fecha de fallo y hasta que la solución sea puesta en producción y haya sido aceptada por la DGTI, asimismo, en la etapa de soporte técnico acudirá a las reuniones generadas bajo demanda por parte del administrador del contrato de la DGTI.

6.10. ADMINISTRADOR DE LA ENTREGA DE LOS SERVICIOS

El proveedor deberá designar desde la puesta en producción de la solución a un Administrador de la entrega de los servicios (SDM por sus siglas en Ingles), el cual deberá contar mínimo con estudios de nivel maestría y deberá estar certificado en ITIL v3, el cual presentará su curriculum vitae y certificaciones vigentes al administrador del contrato designado por la DGTI. Quien actuará en su nombre y representación, dicho recurso residirá en la Ciudad de México o en su zona metropolitana, y será responsable de la administración del contrato por parte del proveedor para la ejecución de los servicios motivo del presente contrato.

El SDM será el único punto de enlace entre la DGTI y el Proveedor una vez que el contrato se encuentre en su etapa productiva, y será responsable brindar la atención oportuna a las peticiones realizadas hacia proveedor.

De tal forma que será el encargado del seguimiento oportuno de los incidentes levantados en la mesa de servicio y de la satisfacción del Cliente, además de las siguientes actividades:

- ✓ Control y gestión las actividades del equipo de trabajo durante la vida del contrato (Ingeniería, Servicios Profesionales, Cliente):
- ✓ Documento de Acuerdos
- ✓ Agendas de entrega de productos y servicios
- ✓ Administración de pendientes
- ✓ Resolución de conflictos
- ✓ Control de entregables
- ✓ Vigilar el cumplimiento de los tiempos comprometidos.
- ✓ Entrega de reportes y generación oportuna de facturación.

Este servicio de SDM será vigente desde la puesta en producción de la solución y hasta el final de la vigencia del contrato y transición del mismo.

7. ENTREGABLES

Al concluir cada una de las implementaciones de las soluciones del proyecto, la documentación requerida en cada una de las actividades deberá haber sido revisada, aceptada, y contar con las firmas autógrafas del personal que la DGTI designe para tal efecto.

Los entregables requeridos en el proyecto deberán ser entregados en formato digital y serán impresos bajo solicitud específica del administrador por parte del INAI. Se firmará un acta como entrega del elemento digital donde se especifique el contenido y cantidad de hojas que componen el mismo, así como un índice de los archivos y su contenido y una copia de la pantalla del mismo tomada en la máquina del administrador del INAI al momento de la entrega.

La DGTI contará con un máximo de 10 (diez) días hábiles para solicitar correcciones a dichos entregables. El Licitante estará obligado a presentar las correcciones la DGTI solicite dentro del marco y alcance del documento correspondiente.

ETAPA	ENTREGABLE	FECHA DE ENTREGA
Etapa 1: Preproductiva	✓ Carta firmada por el representante legal del fabricante y dirigida el INAI (una carta por cada fabricante de cada producto), en donde lo acredite como distribuidor autorizado y que además brindará el soporte y garantía en todos y cada uno de los componentes de la marca ofertada durante la vigencia del contrato.	3 días hábiles posteriores a la notificación del fallo.
	✓ Documento oficial de cumplimiento de la Norma Oficial Mexicana NOM-019-SCFI-1998 relativa a la seguridad de equipo de procesamiento de datos.	10 días hábiles posteriores a la notificación del fallo
	✓ Plan de trabajo final para la implementación de cada una de las soluciones requeridas ✓ Documentación para levantamiento de necesidades que será utilizado por el Proveedor para identificar la información necesaria para implementar cada una de las soluciones alcance de este Anexo Técnico.	A más tardar a los 10 días hábiles posteriores a la notificación del fallo.
	✓ Reportes de la mesa de ayuda: o Propuesta en operación del servicio de mesa de ayuda. o Procedimiento de atención a fallas, el cual deberá contener los medios de contacto o Proceso para solicitar soporte o Directorio de escalamiento con al menos tres niveles	A más tardar a los 10 días hábiles posteriores a la notificación del fallo.
	✓ Evidencia de transferencia de conocimiento	A más tardar 30 días hábiles a partir de la notificación del fallo
Etapa 4: Producción	✓ Memoria Técnica de la implementación de la solución, que contenga al menos: o Solución implementada o Descripción de las especificaciones técnicas o Descripción del producto a nivel funcional o Detalles de la implementación de la correspondiente solución o Consideraciones especiales o Inventario de componentes ✓ Carta de entrega, finalización y aceptación de la implementación de la solución	A más tardar 30 días hábiles posteriores a la finalización de la implementación (Etapa 2) de la solución.
	✓ Reportes mensuales para facturación que deben contener: o Reporte mensual de incidentes. o Disponibilidad de cada uno de los componentes del mes correspondiente.	A más tardar 10 días hábiles posteriores a la finalización de cada mes.

ETAPA	ENTREGABLE	FECHA DE ENTREGA
Etapa 5: Soporte Técnico	✓ Documento de Niveles de servicio y métricas a ser consideradas en el servicio de Soporte Técnico a brindar a la organización, Este documento debe incluir el procedimiento o manual de apertura y registro de incidentes con nombre, teléfono, correo electrónico, línea de escalación y en caso de existir, la referencia de sitios de internet del fabricante de recursos de soporte y conocimientos de apoyo	A más tardar durante la tercera semana a partir del inicio formal de las actividades (Inicio de la etapa 1).

Nota: La revisión por parte de la DGTI de los entregables de cada etapa, se realizará durante los 5 días hábiles posteriores a su entrega, el proveedor contará con un periodo máximo de 5 días hábiles para solventar las observaciones emitidas.

8. NIVELES DE SERVICIO

El servicio especializado de soporte técnico deberá cubrir los siguientes requerimientos:

1) El alcance del servicio especializado de soporte técnico es sobre toda la infraestructura y plataformas que se provean en esta propuesta para cubrir con todos los requerimientos de la DGTI hasta el último día de vigencia del contrato.
2) El servicio especializado de soporte será bajo solicitud expresa de la DGTI hacia la mesa de ayuda del proveedor: en cualquier caso, el servicio deberá ser brindado de manera remota o local, para cumplir con los tiempos comprometidos en el contrato y ante una solicitud o notificación expresa por parte de personal autorizado de la DGTI hacia el proveedor por los conductos autorizados.
3) El servicio debe cubrir lo siguiente:
    a. Soporte para asistencia de requerimientos específicos para cambios de configuración. (Remoto o local)
    b. Apoyo para la actualización de las versiones de plataformas. (Remoto o local).
    c. Atención de consultas de altas, bajas y/o modificación de componentes particulares de las plataformas involucradas. (Remoto)
    d. En el caso de las actualizaciones de versiones de Firmware, hotfixes de seguridad y/o parches, el proveedor notificará a la DGTI de las mismas y un reporte de las implicaciones y los beneficios para su aceptación y programación en conjunto de su ejecución. (Local)
4) El servicio deberá cubrir al menos los siguientes niveles de servicio:

Niveles de severidad:

- **Severidad 1-Crítica:** Un problema grave que le impide llevar a cabo funciones críticas para el instituto.
- **Severidad 2-Alta:** Un incidente que permite llevar a cabo las funciones del trabajo, pero el rendimiento de estas funciones está degradado o extremadamente limitado.
- **Severidad 3-Media:** el rendimiento del trabajo del usuario o grupo de trabajo no se ve prácticamente afectado.
- **Severidad 4-Baja:** Impacto mínimo en el sistema; incluye solicitudes de características y otras preguntas que no se consideran críticas.

Niveles de servicio

i. Soporte técnico telefónico o en línea de acuerdo al nivel de severidad:
   1. 30 minutos, 7 x 24.
   2. 2 horas, 7 x 24.
   3. 3 horas, en horario laborable local.
   4. 8 horas, en horario laborable local.

ii. Soporte en sitio de acuerdo a nivel de severidad:
   1. 4 horas, 7 x 24.
   2. 12 horas naturales.
   3. El siguiente día laboral local.
   4. El siguiente día laboral local.

iii. Entrega de piezas de reemplazo de acuerdo al nivel de severidad:
   1. 5 horas, 7 x 24.
   2. El siguiente día laboral según horario local.
   3. El siguiente día laboral según horario local.
   4. El siguiente día laboral según horario local.

5) Contar con los siguientes canales de atención: vía telefónica, correo electrónico, acceso remoto por VPN, Webex (o similar) y asistencia a sitio cuando se considere necesario por parte del SDM y el Administrador del contrato.
6) Contar con un único punto de contacto para el registro del incidente o problema (mesa de servicio), este podrá recibir el registro vía telefónica, web o correo electrónico.
7) Contar con un sistema de registro de incidentes y asignación y entrega a la organización del mismo ante una notificación o requerimiento de soporte.
8) El servicio en sitio deberá ser brindado en instalaciones del INAI en la Ciudad de México.
9) El servicio especializado de soporte técnico deberá contemplar la gestión del ciclo completo del proceso de reemplazo de equipos ante rotura, así como la puesta en producción del nuevo equipo.

7 GARANTÍAS

El Proveedor para garantizar el cumplimiento de sus obligaciones, deberá otorgar fianza expedida por Institución Autorizada para ello, a favor del INAI, por un importe equivalente al 10% (diez por ciento) sobre el monto máximo del contrato correspondiente, sin considerar el Impuesto al Valor Agregado. Lo anterior, de conformidad con lo establecido en el artículo 48, fracción II, del Reglamento de Adquisiciones, Arrendamiento y Servicios del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Dicha garantía será indivisible deberá presentarse en la Dirección de Recursos Materiales sita en Avenida Insurgentes Sur 3211, Alcaldía, Coyoacán, Col. Insurgentes Cuicuilco, 04530 Ciudad de México, CDMX, dentro de los 10 días naturales posteriores a la firma del contrato correspondiente.

8 DEDUCTIVAS POR INDISPONIBILIDAD DEL SERVICIO

De conformidad con lo establecido en el artículo 53, del Reglamento de Adquisiciones, Arrendamientos y Servicios del INAI, así como el Capítulo XI, numeral 4 de las Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, se aplicará al proveedor las deductivas que se enlistan a continuación, por los servicios prestados de manera parcial o deficiente referentes a la facturación mensual que corresponda, por dichos servicios, teniendo en cuenta que la deductiva no podrá exceder de 8% del monto total del contrato.

Lo anterior, sin perjuicio del derecho que tiene el INAI de optar entre exigir el cumplimiento del contrato o rescindirlo y por lo tanto hacer efectiva la garantía de cumplimiento.

A continuación, se enlista la tabla de deductivas aplicables dependiendo de los tiempos de solución utilizados para cada caso:

Equipo en arrendamiento	Criticidad	Impacto	Tiempo de solución máximo permitido (7x24)	Deductiva aplicable después del tiempo de solución máximo permitido
• **Hardware para Balanceo de Tráfico de internet** • **Hardware para Protección de Aplicaciones WEB** • **Hardware para Seguridad Perimetral** • **Hardware para prevención y detección de intrusos.** • **Hardware detección y protección contra amenazas avanzadas** • **Servicio de protección avanzada para servidores**	Crítica	Interrupción total del servicio	5 hrs	1% de la facturación mensual del equipo afectado por hora de retraso
		Interrupción parcial de los servicios	8 hrs.	1 % de la facturación mensual del equipo afectado por hora de retraso
		Falla de una parte que no interrumpe el servicio	24 hrs.	1% de la facturación mensual del equipo afectado por día de retraso
• **Hardware para Balanceo de Tráfico** • **Hardware para Protección de**	Alta	Interrupción total del servicio	24 hrs	1% de la facturación mensual del equipo afectado por hora de retraso
		Interrupción parcial de los servicios	28 hrs.	1% de la facturación mensual del equipo afectado por hora de retraso

Equipo en arrendamiento	Criticidad	Impacto	Tiempo de solución máximo permitido (7x24)	Deductiva aplicable después del tiempo de solución máximo permitido
Aplicaciones WEB • **Hardware para Seguridad Perimetral** • **Hardware para prevención y detección de intrusos.** • **Hardware detección y protección contra amenazas avanzadas** • **Servicio de protección avanzada para servidores**		Falla de una parte que no interrumpe el servicio	36 hrs.	1% de la facturación mensual del equipo afectado por día de retraso
• **Hardware para Balanceo de Tráfico** • **Hardware para Protección de Aplicaciones WEB** • **Hardware para Seguridad Perimetral** **Hardware para prevención y detección de intrusos.** **Hardware detección y protección contra amenazas avanzadas Servicio de protección avanzada para servidores**	Media	Interrupción total del servicio	26 hrs	1% de la facturación mensual del equipo afectado por hora de retraso
		Interrupción parcial de los servicios	30 hrs.	1% de la facturación mensual del equipo afectado por hora de retraso
		Falla de una parte que no interrumpe el servicio	38 hrs.	1% de la facturación mensual del equipo afectado por día de retraso
• **Hardware para Balanceo de Tráfico** • **Hardware para Protección de**	Baja	Interrupción total del servicio	28 hrs	1% de la facturación mensual del equipo afectado por hora de retraso
		Interrupción parcial de los servicios	34 hrs.	1% de la facturación mensual del equipo afectado por hora de retraso

Equipo en arrendamiento	Criticidad	Impacto	Tiempo de solución máximo permitido (7x24)	Deductiva aplicable después del tiempo de solución máximo permitido
Aplicaciones WEB • **Hardware para Seguridad Perimetral** • **Hardware para prevención y detección de intrusos.** • **Hardware detección y protección contra amenazas avanzadas** • **Servicio de protección avanzada para servidores**		Falla de una parte que no interrumpe el servicio	42 hrs.	1% de la facturación mensual del equipo afectado por día de retraso

Nota: el tiempo expresado en la tabla anterior será considerado en horas naturales

9 PENAS CONVENCIONALES

Las penas convencionales se determinarán en función de los servicios no prestados oportunamente, a razón del 1% (uno por ciento) diario sobre el precio mensual de los mismos antes de IVA, por cada día natural de atraso y esta se hará efectiva con cargo al importe de los servicios pendientes de pago.

Lo anterior con fundamento en lo establecido en el Capítulo XI "Del seguimiento a los contratos y pedidos", Numeral 3 "De la aplicación de penas convencionales", séptimo párrafo de las "Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales" (BALINES-INAI); sin perjuicio del derecho que tiene el INAI de optar entre exigir el cumplimiento del contrato o rescindirlo y por lo tanto hacer efectiva la garantía de cumplimiento.

En todos los casos, las penas no deberán exceder de manera conjunta referente a la disponibilidad de atención y solución de incidentes, del 10% como monto total del contrato.

Lo anterior no exime de la responsabilidad de mantener operativos los servicios hasta que se halla migrado la totalidad de los servicios.

10 INFORMACIÓN ADMINISTRATIVA

10.1 CUMPLIMIENTO DE NORMAS

En esta contratación se requiere el cumplimiento de la Norma Oficial Mexicana NOM-019-SCFI-1998 relativa a la seguridad de equipo de procesamiento de datos,

El proveedor deberá acreditar esta NOM presentando el documento oficial de cumplimiento de la misma y esta solo aplicará a los equipos que sean contemplado para la prestación del servicio.

El proveedor deberá entregar estas evidencias a más tardar 10 días hábiles posteriores a la notificación del fallo.

10.2 SEGUROS

Será responsabilidad única y exclusiva del proveedor obtener y mantener a su costo, una póliza de seguro para todos los equipos necesarios para la prestación de los servicios, la cual será presentada antes de iniciar la fase de implementación al administrador del contrato que designe la DGTI.

10.3 ASPECTOS ECONÓMICOS

Por ningún motivo se otorgarán anticipos.

El pago se realizará a mes vencido en una sola exhibición. El trámite para generar el pago sólo podrá iniciarse a partir de la fecha en que el responsable de administrar el contrato por parte de la DGTI, haya recibido a su entera satisfacción los entregables conforme la tabla del numeral 7.

Dicho pago se efectuará dentro de los 20 días naturales contados a partir de la entrega de la factura a la Dirección General de Administración, misma que deberá cumplir con los requisitos establecidos en el Código Fiscal de la Federación, en el entendido de que si la factura presenta alguna deficiencia se devolverá al proveedor para su corrección, prorrogándose el plazo para su pago en los mismos días en que se efectúen dichas correcciones y sea nuevamente entregada (artículo 50 primer párrafo, Reglamento).

Los pagos se tramitarán conforme a la normatividad vigente y se efectuarán en moneda nacional, mensualmente con base en la recepción de los productos y servicios a entera satisfacción de la Dirección General de Tecnologías de la Información del INAI.

Las propuestas deben presentarse en moneda nacional. Las cotizaciones deben de considerar los costos unitarios de cada producto con base en el siguiente formato:

Descripción del bien y/o servicio	Unidad	Cantidad*	Precio Unitario	Total
Hardware para Balanceo de Tráfico	Pieza	2	1,263,824.44	2,527,648.88
Hardware para protección de aplicaciones web.	Pieza	2	1,981,899.33	3,963,798.66
Hardware para Seguridad Perimetral	Pieza	2	2,204,796.36	4,409,592.71
Hardware para Prevención de Intrusos.	Pieza	2	6,468,056.33	12,936,112.67
Hardware para detección y protección contra amenazas avanzadas.	Pieza	1	2,902,541.23	2,902,541.23
Servicio de protección avanzada para servidores	licencia	10	24,130.59	241,305.85
			Subtotal	26,981,000.00
			IVA	4,316,960.00
			Total	31,297,960.00

* **NOTA:** Toda vez que el arrendamiento será mediante un contrato abierto, las cantidades de equipos son demostrativas para que los licitantes puedan presentar sus ofertas económicas.

LEÍDO EL PRESENTE INSTRUMENTO Y ENTERADAS LAS PARTES DE SU CONTENIDO Y ALCANCE DE TODAS LAS CLÁUSULAS, LO FIRMAN EN CINCO TANTOS ORIGINALES EN LA CIUDAD DE MÉXICO, A LOS DIECINUEVE DÍAS DEL MES DE DICIEMBRE DEL AÑO 2019----------

POR EL "INAI"

ING. JOSÉ LUIS HERNÁNDEZ SANTANA
DIRECTOR GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN

POR EL "PROVEEDOR"

SELENE ELIZABETH CASTAÑON GUTIERREZ
REPRESENTANTE LEGAL

ÚLTIMA HOJA DEL CONTRATO DE PRESTACIÓN DE ARRENDAMIENTO SIN OPCIÓN A COMPRA, QUE CELEBRAN EL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES Y GRUPO DE TECNOLOGÍA CIBERNÉTICA, S.A. DE C.V. CELEBRADO EN LA CIUDAD DE MÉXICO, EL 6 DE DICIEMBRE DE 2019. ----------