



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

CONTRATO PARA LA PRESTACIÓN DEL "SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA", EN ADELANTE "EL SERVICIO", QUE CELEBRAN POR UNA PARTE LA COMISIÓN EJECUTIVA DE ATENCIÓN A VÍCTIMAS, EN LO SUCESIVO "LA CEAV", REPRESENTADA EN ESTE ACTO POR EL C.P. SALVADOR OSOGOBIO VILLEGAS, DIRECTOR DE RECURSOS MATERIALES Y SERVICIOS GENERALES DE "LA CEAV", Y EL ING. ROGELIO MESTA ESTRADA, EN SU CARÁCTER DE DIRECTOR DE TECNOLOGÍAS DE LA INFORMACIÓN DE "LA CEAV", A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ "EL ADMINISTRADOR DEL CONTRATO" Y POR LA OTRA, ORBEN COMUNICACIONES S.A.P.I. DE C.V., REPRESENTADA POR EL C. CRISTÓBAL ERNESTO GARCÍA VEGA, EN SU CARÁCTER DE APODERADO LEGAL, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ "EL PROVEEDOR", Y A QUIENES CUANDO SE HAGA REFERENCIA DE MANERA CONJUNTA SE LES DENOMINARÁ "LAS PARTES", AL TENOR DE LAS DECLARACIONES Y CLÁUSULAS SIGUIENTES:

DECLARACIONES

1. **"LA CEAV"** declara que:

- 1.1 Es un Organismo con personalidad jurídica y patrimonio propios; con autonomía técnica, de gestión y contará con los recursos que le asigne el Presupuesto de Egresos de la Federación, de conformidad con el artículo 84 de la Ley General de Víctimas, última reforma publicada en el Diario Oficial de la Federación el 3 de enero de 2017.
- 1.2 El C.P. Salvador Osogobio Villegas, en su carácter de Director de Recursos Materiales y Servicios Generales de **"LA CEAV"**, tiene facultades para suscribir el presente Contrato, de conformidad con los artículos 5, fracción XI inciso c; 23 bis párrafo segundo y 34 fracción XVIII del Estatuto Orgánico de **"LA CEAV"**, última reforma publicada en el Diario Oficial de la Federación el 20 de diciembre de 2018.
- 1.3 El Ing. Rogelio Mesta Estrada, en su carácter de Director de Tecnologías de la Información de **"LA CEAV"**, o quien lo sustituya o supla, serán responsables de administrar, validar y supervisar el cabal cumplimiento del presente Contrato y su **Anexo I** en su calidad de **"EL ADMINISTRADOR DEL CONTRATO"**, de conformidad con lo establecido en el artículo 84, séptimo párrafo del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
- 1.4 Este Contrato se celebra mediante el procedimiento de Adjudicación Directa con fundamento en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos; 25, primer párrafo, 26 fracción III, 41, fracción



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

V y 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; 72, fracción V y 85 de su Reglamento y demás disposiciones relativas y aplicables vigentes.

El procedimiento de contratación fue dictaminado procedente, mediante escrito de justificación de fecha 29 de noviembre de 2019, signado por **"EL ADMINISTRADOR DEL CONTRATO"**, y autorizado mediante dictamen de procedencia, de fecha 29 de noviembre de 2019, signado por C.P. Salvador Osogobio Villegas, Director de Recursos Materiales y Servicios Generales, en suplencia por el Titular de la Dirección General de Administración y Finanzas conforme a los artículos 5, fracción XI inciso c; 23 bis párrafo segundo y 34 fracción XVIII del Estatuto Orgánico de **"LA CEAV"**, notificándose la adjudicación mediante oficio número CEAV/DGAYF/DRMSG/1784/2019 de fecha 29 de noviembre de 2019.

- 1.5 Con fundamento en los artículos 2, fracción XVI, 5, fracción II, mediante oficio número CEAV/DGAYF/1870/2019, de fecha 28 de agosto de 2019, signado por la Mtra. Elba Matilde Loyola Orduña, en ese entonces, Directora General de Administración y Finanzas de **"LA CEAV"**, se autorizó la disponibilidad del recurso del presupuesto aprobado para la partida presupuestal número 31904 "Servicios integrales de infraestructura de cómputo", para iniciar el proceso de adjudicación directa, para la contratación de **"EL SERVICIO"** materia del presente instrumento jurídico.
 - 1.6 Cuenta con autorización para el proceso de contratación plurianual, lo que acredita con el oficio CEAV/DGAYF/1879/2019, de fecha 29 de agosto de 2019, signado por la Mtra. Elba Matilde Loyola Orduña, en ese entonces, Directora General de Administración y Finanzas de **"LA CEAV"**, autoriza el proceso para la contratación plurianual objeto del presente Contrato, contándose con el registro en el Módulo de Administración y Seguimiento de Contrato Plurianuales (MASCP), con número de folio **2019-47-AYJ-19**.
 - 1.7 Su Registro Federal de Contribuyentes es PSA110907866.
 - 1.8 Para efectos del presente Contrato tiene su domicilio legal, el ubicado en Avenida Ángel Urraza 1137, Colonia Del Valle, Alcaldía Benito Juárez, C.P. 03100, en la Ciudad de México.
2. **"EL PROVEEDOR"** declara que:
- 2.1 Es una sociedad mercantil que está legalmente constituida conforme a las Leyes Mexicanas, de conformidad con la escritura pública número 5,252, de fecha 02 de abril de 1998, otorgada ante la fe del Notario Público número 44 de la Ciudad de Monterrey, capital del Estado de Nuevo León, el Licenciado



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

Arnulfo Flores Rodríguez, inscrita en el Registro Público de la Propiedad y del Comercio del Primer Distrito Monterrey, Nuevo León, bajo el folio mercantil número 1124, constituyéndose como ORBEN COMUNICACIONES, S.A. DE C.V.; mediante escritura pública número 10,834, de fecha 01 de octubre de 2013, otorgada ante la fe del Notario Público número 69 del Primer Distrito registral en el Estado de Nuevo León, Licenciado y Contador Público César González Cantú, inscrita en el Registro Público de la Propiedad y del Comercio Monterrey, Nuevo León, bajo el folio mercantil electrónico número 63034*9, en la que protocoliza el Acta de Asamblea General Extraordinaria de accionistas, se llevó a cabo la transformación de la sociedad para adoptar la modalidad de Sociedad Anónima Promotora de Inversión de Capital Variable, para queda como ORBEN COMUNICACIONES, S.A.P.I. DE C.V., reformando íntegramente sus estatutos sociales.

- 2.2** Su objeto es entre otros, la compra, venta, distribución de equipos y accesorios para informática y telecomunicaciones; la asesoría, consultoría, venta, renta, capacitación y prestación de toda clase de servicios, por cuenta propia o de terceros, a todas clase de personas, empresas e instituciones, así como el gobierno federal, estatal y/o municipal, organismos descentralizados, entidades paraestatales, empresas de participación estatal mayoritaria, fideicomisos públicos, en las áreas de telecomunicaciones, programación, computación y sistemas, aplicaciones móviles, redes sociales, internet, así como en las áreas de administración, consultoría en mercadotecnia y ventas, asuntos pedagógicos, informáticos de cobranza, diseño industrial, gráfico y urbano, proyectos de infraestructura, construcción, estudios de inversión, contratos, plantación, dirección, administración, auditoría, importaciones, exportaciones, recursos humanos, análisis, diseño e implementación de programas, producción, sistemas mercadotecnia, publicad, estudios de factibilidad, entre otros, así como la promoción, fomento y comercialización de todo tipo de bienes y servicios y comercialización de servicios de telecomunicaciones nacional e internacional.
- 2.3** El C. Cristóbal Ernesto García Vega, Apoderado legal, quien se identifica con credencial para votar con clave de elector número [REDACTED] expedida a su favor por el Instituto Nacional Electoral, cuenta con las facultades suficientes para suscribir el presente Contrato, y acredita su personalidad con el instrumento número 57,932, de fecha 30 de noviembre de 2016, pasada ante la fe del Notario Público número 18 del Distrito Federal, ahora Ciudad de México, el Licenciado Patricio Garza Bandala actuando como asociado de la Licenciada Ana Patricia Bandala Tolentino, Notaria número 195 del Distrito Federal, ahora Ciudad de México, inscrito en el Registro Público de la Propiedad y de Comercio de Monterrey, Estado de Nuevo León, bajo el folio mercantil número 63034, mismas que a la fecha de



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

suscripción del presente Contrato no le han sido modificadas, limitadas o revocadas en forma alguna.

- 2.4** En atención al artículo 32-D del Código Fiscal de la Federación, a la regla 2.1.31. de la Resolución Miscelánea Fiscal para 2018, presentó documento actualizado, emitido por el Servicio de Administración Tributaria (SAT) de fecha 04 de noviembre de 2019, mediante el cual remite opinión en sentido positivo.
- 2.5** En cumplimiento a las Reglas para la Obtención de la Opinión de Cumplimiento de Obligaciones Fiscales en Materia de Seguridad Social, publicadas en el Diario Oficial de la Federación el 27 de febrero del 2015, así como su actualización publicada en el Diario Oficial de la Federación, el 3 de abril de 2015, presentó documento actualizado, emitido por el Instituto Mexicano del Seguro Social (IMSS) de fecha 27 de noviembre de 2019, mediante el cual remite opinión en sentido positivo.

Asimismo, en atención al Acuerdo del H. Consejo de Administración del Instituto del Fondo Nacional de la Vivienda para los Trabajadores por el que se emiten las Reglas para la obtención de la constancia de situación fiscal en materia de aportaciones patronales y entero de descuentos, presenta la constancia de situación fiscal en materia de aportaciones y amortizaciones patronales de fecha 29 de noviembre de 2019, mediante el cual se advierte que ORBEN COMUNICACIONES, S.A.P.I. DE C.V., con Número de Registro Patronal Y3723252106, NO se identificaron adeudos ante el INFONAVIT, mismo que se encuentra al corriente de sus obligaciones que señala el artículo 29 de la Ley del Instituto del Fondo Nacional de la Vivienda para los Trabajadores, de aportar el cinco por ciento de los salarios cubiertos a sus trabajadores y de retener y enterar los descuentos para amortizaciones de crédito, hasta el 04 bimestre 2019.

- 2.6** Mediante escrito de fecha 29 de noviembre de 2019, manifiesta bajo protesta de decir verdad, que la estratificación que le corresponde es empresa MEDIANA, de conformidad con lo establecido en el ACUERDO por el que se establece la estratificación de las micro, pequeñas y medianas empresas, publicado en el Diario Oficial de la Federación con fecha 30 de junio de 2009.

Lo anterior, en términos del artículo 34 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

- 2.7** Mediante escrito de fecha 29 de noviembre de 2019, manifiesta bajo protesta de decir verdad, que no se encuentra bajo los supuestos de los artículos 50 y 60 de Ley de Adquisiciones, Arrendamientos y Servicios del



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

Sector Público, vinculados con lo previsto en el artículo 49, fracción IX de la Ley General de Responsabilidades Administrativas.

- 2.8** Su Registro Federal de Contribuyentes es OCO9804024E6.
- 2.9** Para los efectos del presente contrato señala como su domicilio legal, el ubicado en Calle José Benítez, número 606, Colonia Obispado, Monterrey, C.P. 64060, en Nuevo León.

Enteradas "**LAS PARTES**" de las declaraciones anteriores, acuerdan suscribir el presente Contrato, al tenor de las siguientes:

CLÁUSULAS

PRIMERA.- OBJETO. El objeto del presente Contrato lo constituye la obligación de "**EL PROVEEDOR**" de proporcionar a favor de "**LA CEAV**", de la infraestructura de comunicaciones (SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA) necesaria para ofrecer una mejor conectividad entre las diferentes oficinas de "**LA CEAV**" optimizando la transmisión de datos, así como incrementar la seguridad en todos los puntos de las comunicaciones de la red de "**LA CEAV**", a través de un servicio administrado de red de voz, datos y seguridad, de conformidad con las especificaciones, requerimientos, alcances y características técnicas contenidas en las cláusulas de este Contrato y sus **Anexos**:

Anexo I: Términos de Referencia.

Anexo II: Propuesta Económica de "**EL PROVEEDOR**".

SEGUNDA.- MONTO. En términos de los artículos 47 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 85 de su Reglamento, los montos que "**LA CEAV**" pagará a "**EL PROVEEDOR**", para los ejercicios fiscales 2019 y 2020, serán los siguientes:

Montos durante el ejercicio fiscal 2019

"**LA CEAV**" pagará a "**EL PROVEEDOR**", durante el ejercicio 2019, el monto mínimo de \$75,862.07 (Setenta y cinco mil ochocientos sesenta y dos pesos 07/100 M.N.), más \$12,137.93 (Doce mil ciento treinta y siete pesos 93/100 M.N.), correspondientes al 16% del L.V.A., resultando la cantidad total de \$88,000.00 (Ochenta y ocho mil pesos 00/100 M.N.) y el monto máximo que "**LA CEAV**" pagará a "**EL PROVEEDOR**", será de \$189,655.17 (Ciento ochenta y nueve mil seiscientos cincuenta y cinco pesos 17/100 M.N.), más \$30,344.83 (Treinta mil trescientos cuarenta y cuatro pesos 83/100 M.N.), correspondientes al 16% del



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

I.V.A., resultando la cantidad total de \$220,000.00 (Doscientos veinte mil pesos 00/100 M.N.).

Montos durante el ejercicio fiscal 2020

"LA CEAV" pagará a "EL PROVEEDOR", durante el ejercicio fiscal 2020, el monto mínimo de \$841,379.31 (Ochocientos cuarenta y un mil trescientos setenta y nueve pesos 31/100 M.N.), más \$134,620.69 (Ciento treinta y cuatro mil seiscientos veinte pesos 69/100 M.N.), correspondientes al 16% del I.V.A., resultando la cantidad total de \$976,000.00 (Novecientos setenta y seis mil pesos 00/100 M.N.) y el monto máximo que "LA CEAV" pagará a "EL PROVEEDOR", será de \$2'103,448.28 (Dos millones ciento tres mil cuatrocientos cuarenta y ocho pesos 28/100 M.N.), más \$336,551.72 (Trescientos treinta y seis mil quinientos cincuenta y un pesos 72/100 M.N.), correspondientes al 16% del I.V.A., resultando la cantidad total de \$2'440,000.00 (Dos millones cuatrocientos cuarenta mil pesos 00/100 M.N.).

"LA CEAV" pagará a "EL PROVEEDOR", por los ejercicios fiscales 2019 y 2020, un monto mínimo de \$917,241.38 (Novecientos diecisiete mil doscientos cuarenta y un pesos 38/100 M.N.), más \$146,758.62 (Ciento cuarenta y seis mil setecientos cincuenta y ocho pesos 62/100 M.N.), correspondientes al 16% del I.V.A., resultando la cantidad total de \$1'064,000.00 (Un millón sesenta y cuatro mil pesos 00/100 M.N.) y el monto máximo que "LA CEAV" pagará a "EL PROVEEDOR", será de \$2'293,103.45 (Dos millones doscientos noventa y tres mil ciento tres pesos 45/100 M.N.), más \$366,896.55 (Trescientos sesenta y seis mil ochocientos noventa y seis pesos 55/100 M.N.), correspondientes al 16% del I.V.A., resultando la cantidad total de \$2'660,000.00 (Dos millones seiscientos sesenta mil pesos 00/100 M.N.).

"LA CEAV" pagará únicamente el Impuesto al Valor Agregado, de conformidad con las disposiciones fiscales vigentes.

"EL PROVEEDOR" deberá sostener los precios pactados tal como se muestra en el **Anexo II** del presente Contrato, sin modificación alguna durante su vigencia y hasta su vencimiento; dichos precios incluyen todos los conceptos que "EL SERVICIO" requiere, por lo que "EL PROVEEDOR" no podrá agregar ningún costo extra, siendo inalterables durante la vigencia del Contrato.

Dichos precios son cotizados en moneda nacional, fijos y no estarán sujetos a ajustes.

TERCERA.- TIEMPO Y FORMA DE PAGO. En términos del artículo 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el pago se realizará de conformidad con "EL SERVICIO" efectivamente prestado, previa



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

comprobación, verificación y aceptación del mismo por **"EL ADMINISTRADOR DEL CONTRATO"**.

Los pagos se realizarán de manera mensual, en moneda nacional de conformidad con **"EL SERVICIO"** prestado, dentro de los 20 (veinte) días naturales posteriores a la presentación del comprobante fiscal digital respectivo, el cual deberá cumplir con los requisitos fiscales vigentes, previa conformidad de **"EL ADMINISTRADOR DEL CONTRATO"**. Los pagos, se efectuarán mediante transferencia electrónica, por lo que **"EL PROVEEDOR"** deberá presentar documento expedido por institución bancaria.

Para efectos de lo anterior, **"EL ADMINISTRADOR DEL CONTRATO"** deberá remitir a la Dirección General de Administración y Finanzas de **"LA CEAV"**, la documentación en original que compruebe la prestación de **"EL SERVICIO"** junto con el comprobante fiscal digital correspondiente en la que manifieste su entera satisfacción respecto a la prestación de **"EL SERVICIO"**, en tiempo y forma, solicitando por escrito que se tramite el pago. En su caso, cuando **"EL SERVICIO"** sea prestado de forma parcial o deficiente o exista algún atraso en la prestación del mismo, será responsabilidad de **"EL ADMINISTRADOR DEL CONTRATO"** determinar el importe que se aplicará por concepto de penas convencionales, documentarlas, así como notificar por escrito a la Dirección General de Administración y Finanzas de **"LA CEAV"** el importe de las mismas.

En caso de que el comprobante fiscal digital y/o documentación presente errores o deficiencias, **"LA CEAV"**, dentro de los 3 días hábiles siguientes al de su recepción, indicará por escrito las inconsistencias que se deberán corregir y devolverá la documentación a **"EL PROVEEDOR"** para que sea subsanada y la presente nuevamente para reiniciar el trámite de pago, cuyo plazo para realizarse se computará a partir de la fecha de presentación de la documentación corregida, que no deberá exceder de 3 días naturales contados a partir de la fecha de su devolución, de conformidad con lo establecido en los artículos 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; así como 89 y 90 de su Reglamento.

Los trámites de pago correspondientes, se efectuarán con los siguientes datos fiscales: a nombre de la Comisión Ejecutiva de Atención a Víctimas, con el domicilio fiscal siguiente: Avenida Ángel Urraza núm. 1137, Colonia Del Valle, Alcaldía Benito Juárez, Ciudad de México, C.P. 03100, con el Registro Federal de Contribuyentes PSA110907866, y deberá ser enviado el comprobante fiscal digital por vía electrónica para su validación, al correo electrónico que señale **"EL ADMINISTRADOR DEL CONTRATO"**.

Los pagos de **"EL SERVICIO"**, quedarán condicionados al pago que **"EL PROVEEDOR"** deba efectuar por concepto de penas convencionales que se



CEAV
COMISION EJECUTIVA
DE ATENCION A VICTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

determinen conforme a lo que establece la cláusula **DÉCIMA CUARTA** del presente Contrato.

CUARTA.- VIGENCIA. La vigencia del presente Contrato iniciará a las 00:00 horas del día 20 de diciembre de 2019 y concluirá a las 23:59 horas del día 30 de abril de 2020.

QUINTA.- ANTICIPO. En la presente contratación, "**LA CEAV**" no otorgará anticipos.

SEXTA.- PAGOS EN EXCESO. En caso de que existan pagos en exceso que haya recibido "**EL PROVEEDOR**", deberá reintegrarlos, así como pagar los intereses correspondientes conforme a la tasa que será igual a la establecida por la Ley de Ingresos de la Federación en los casos de prórroga para el pago de créditos fiscales. 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 en que se pongan efectivamente las cantidades a disposición de "**LA CEAV**".

SÉPTIMA.- GARANTÍA DE CUMPLIMIENTO DEL CONTRATO.

- 1) **DEL CUMPLIMIENTO DEL CONTRATO. "EL PROVEEDOR"**, a fin de garantizar el cumplimiento de las obligaciones derivadas del Contrato y de conformidad con los artículos 48, fracción II y 49, fracción II de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; 103 de su Reglamento; y 48 de la Ley de Tesorería de la Federación se compromete a:
 - A) Otorgar una garantía de cumplimiento por una cantidad equivalente al 10% del monto máximo de este Contrato antes del Impuesto al Valor Agregado, en pesos mexicanos e idioma español, en alguna de las formas previstas en el artículo 48 de la Ley de Tesorería de la Federación, preferentemente a través de fianza.
 - B) Deberá presentar escrito en hoja membretada y firmado por "**EL PROVEEDOR**" en donde ofrezca y exhiba la garantía de cumplimiento, a más tardar dentro de los 10 días naturales siguientes a la firma del Contrato, misma que deberá ser entregada en la Dirección de Recursos Materiales y Servicios Generales, a través del área de contratos, sita en Avenida Ángel Urraza número 1137, piso 2, Colonia Del Valle, Alcaldía Benito Juárez, C.P. 03100, en la Ciudad de México, en un horario de lunes a viernes de 9:00 a 14:00 horas. La falta de presentación de la garantía o de cumplimiento en el plazo concedido, dará como consecuencia el inicio del procedimiento de rescisión por incumplimiento de los requerimientos para formalizar el Contrato.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA

- C) Que la vigencia de la garantía de cumplimiento, deberá quedar abierta para permitir que cumpla con su objetivo, de forma tal que no podrá establecer o estipularse plazo alguno que limite su vigencia, lo cual no deberá confundirse con los plazos para el cumplimiento de las obligaciones previstas en el Contrato.
- 2) Cuando la forma de garantía de cumplimiento sea mediante fianza deberá ser expedida a favor de **"LA CEAV"**, por una institución autorizada en los términos de la Ley de Instituciones de Seguros y de Fianzas y contener, como mínimo, de conformidad con lo establecido en el artículo 103, fracción I, del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, los siguientes requisitos:
- 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, emitida por **"EL ADMINISTRADOR DEL CONTRATO"** o a quien lo sustituya o supla;
 - 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 Institución de fianzas acepta expresamente someterse al procedimiento de ejecución establecido en el artículo 282 de la Ley de Instituciones de Seguros y de Fianzas para la efectividad de la presente garantía, procedimiento al que también se sujetará para el caso de cobro de intereses que prevé el artículo 283 del mismo ordenamiento legal por pago extemporáneo del importe de la póliza de fianza requerida.
- 3) En caso de otorgamiento de prórrogas o esperas a **"EL PROVEEDOR"** para el cumplimiento de sus obligaciones, derivadas de la formalización de convenios de ampliación al monto o al plazo del Contrato, se deberá realizar la modificación correspondiente a la garantía de cumplimiento, en el caso de fianza mediante el endoso correspondiente.
- 4) Cuando al realizarse el finiquito resulten saldos a cargo de **"EL PROVEEDOR"** este efectúe la totalidad del pago en forma incondicional, **"LA CEAV"** deberá cancelar la garantía de cumplimiento respectiva.

"EL PROVEEDOR" acepta expresamente que la garantía expedida para garantizar el cumplimiento se hará efectiva de manera indivisible



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

independientemente de que se interponga cualquier tipo de recurso ante instancias del orden administrativo o judicial, así como que permanecerá vigente durante la substanciación de los juicios o recursos legales que interponga con relación a dicho instrumento jurídico, hasta que sea pronunciada resolución definitiva que cause ejecutoria por la Autoridad competente.

OCTAVA.- OBLIGACIONES Y RESPONSABILIDADES DE "EL PROVEEDOR". Para el cumplimiento del presente Contrato **"EL PROVEEDOR"** se compromete a:

1. Prestar **"EL SERVICIO"** objeto del presente Contrato, de conformidad con las especificaciones, requerimientos, alcances y características técnicas citadas en el presente Contrato y en su **Anexo I**, mismos que debidamente firmados por **"LAS PARTES"** forman parte integrante de este Contrato.
2. Cumplir con las disposiciones legales, reglamentarias, administrativas y en general, con todas las que sean aplicables. Asimismo, responderá ante **"LA CEAV"** por cualquier daño o perjuicio que resultare por el incumplimiento de las mismas.
3. Responder respecto de la calidad de **"EL SERVICIO"** en los términos establecidos en el presente Contrato, así como en su **Anexo I** y en la legislación aplicable.
4. Informar oportunamente a **"LA CEAV"** de los hechos y razones debidamente justificados que lo imposibiliten para cumplir, en su caso, con las obligaciones que le señala el presente Contrato y su **Anexo I**, a efecto de que ésta determine lo conducente conforme a lo previsto en el Contrato y las disposiciones aplicables.
5. Ser el único responsable cuando **"EL SERVICIO"** objeto del presente Contrato, no se haya realizado de acuerdo a lo estipulado en el mismo, por lo que **"LA CEAV"** podrá ordenar la corrección de **"EL SERVICIO"**, sin que **"EL PROVEEDOR"** tenga derecho a retribución adicional alguna por ello, ya que ésta se hará por cuenta de **"EL PROVEEDOR"** en el plazo que para tal efecto se señale. Lo anterior, sin perjuicio de las sanciones que en su caso correspondan, en términos de las cláusulas **DÉCIMA CUARTA** y **DÉCIMA QUINTA** de este Contrato.
6. En caso de realizar servicios excedentes o por mayor valor de lo establecido en este Contrato, sin que para tales efectos se hubiera obtenido la autorización de **"LA CEAV"** y sin que se hubiere celebrado el convenio modificadorio respectivo, independientemente de la responsabilidad en que incurra por la ejecución de **"EL SERVICIO"**, no tendrá derecho a reclamar pago adicional alguno por ello.
7. Contar con todas las autorizaciones requeridas por las instituciones gubernamentales competentes, para la adecuada ejecución del Contrato, por lo que también se obliga a cumplir y realizar **"EL SERVICIO"** en estricto apego con todas las leyes, reglamentos y normas aplicables, sean éstas municipales, estatales o federales.



CEAV

COMISION EJECUTIVA
DE ATENCION A VICTIMAS

CEAV-C-56-2019

SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA

8. Entregar la garantía de cumplimiento solicitada, de conformidad con los términos, plazos y formas establecidos en el presente Contrato.
9. Ser responsable de cualquier daño o afectación que por negligencia, error o dolo, pudiera causar a terceros en su persona o bienes, con motivo de la prestación de **"EL SERVICIO"**.
10. Presentar a la Secretaría de la Función Pública y/o al Órgano Interno de Control de **"LA CEAV"**, con motivo de las auditorías, visitas o inspecciones que practiquen, la información y documentación relacionada con el objeto del presente Contrato, de conformidad con los artículos 57 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 107 de su Reglamento.

NOVENA.- OBLIGACIONES DE "LA CEAV". "LA CEAV" se obliga a:

1. Cubrir el pago de **"EL SERVICIO"** efectivamente prestado de acuerdo a las condiciones y términos estipulados en las cláusulas **SEGUNDA** y **TERCERA** del presente Contrato.
2. Proporcionar a **"EL PROVEEDOR"** las facilidades necesarias para la prestación de **"EL SERVICIO"** materia del presente Contrato.
3. Que a través de **"EL ADMINISTRADOR DEL CONTRATO"**, o quien lo sustituya o supla, serán responsables de administrar, validar y supervisar el cabal cumplimiento de **"EL SERVICIO"**, de acuerdo a lo solicitado en el **Anexo I**.

DÉCIMA.- LUGAR Y CONDICIONES PARA LA PRESTACIÓN DE "EL SERVICIO". **"EL PROVEEDOR"** deberá prestar **"EL SERVICIO"** objeto del presente contrato, en los domicilios señalados en el **Apéndice II** del **Anexo I** de este Contrato, siendo éstos sitios enunciativos más no limitativos y podrán tener modificaciones de acuerdo a las necesidades de **"LA CEAV"**. Asimismo, **"EL SERVICIO"** se prestará conforme a las condiciones y características establecidas en el numeral 3 del **Anexo I** de este Contrato.

DÉCIMA PRIMERA.- VERIFICACIÓN Y COMPROBACIÓN DE "EL SERVICIO". De conformidad con lo previsto por los artículos 84, penúltimo y último párrafo y 108 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, **"EL ADMINISTRADOR DEL CONTRATO"**, deberá verificar y comprobar el cumplimiento de **"EL SERVICIO"**, y estará facultado para recibirlo, aceptarlo a satisfacción y determinar los incumplimientos, conforme a los procedimientos establecidos en el presente Contrato y su **Anexo I**, y deberá comunicar por escrito a **"EL PROVEEDOR"**, las observaciones que estime pertinentes en relación con su ejecución, o bien la aceptación del mismo, lo que tendrá que realizar de acuerdo a lo establecido en el presente Contrato y su **Anexo I**.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

La verificación de **"EL SERVICIO"** que realice **"LA CEAV"**, no libera a **"EL PROVEEDOR"** del cumplimiento de las obligaciones contraídas en este Contrato, así como de las deficiencias que aparezcan posteriormente una vez concluido el mismo. Lo anterior, en el entendido de que el ejercicio de esta facultad, no será considerada como aceptación tácita o expresa de **"EL SERVICIO"**.

"LA CEAV", quedará facultada para realizar visitas físicas a las instalaciones de **"EL PROVEEDOR"** durante la vigencia del Contrato, para lo cual deberá brindar al personal de **"LA CEAV"**, previa identificación del mismo, las facilidades necesarias.

De conformidad con el artículo 57 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, la Secretaría de la Función Pública, podrá realizar las visitas e inspecciones que estime necesarias, así como verificar la calidad de **"EL SERVICIO"** establecido en el presente Contrato, pudiendo solicitar a **"LA CEAV"** y a **"EL PROVEEDOR"** todos los datos e informes relacionados con los actos de que se trate.

DÉCIMA SEGUNDA.- PROCEDIMIENTOS PARA LA VERIFICACIÓN, ACEPTACIÓN O CORRECCIÓN DE "EL SERVICIO". En términos de lo dispuesto por la cláusula que antecede la verificación, aceptación o corrección de **"EL SERVICIO"** se realizará por **"EL ADMINISTRADOR DEL CONTRATO"** conforme a lo siguiente:

El cómputo del plazo entre el momento en el que se presta **"EL SERVICIO"** y el momento en que éste es recibido a satisfacción, se interrumpirá cuando **"EL ADMINISTRADOR DEL CONTRATO"** acredite haber comunicado a **"EL PROVEEDOR"**, en los términos previstos en el **Anexo I** de este Contrato el incumplimiento en la prestación de **"EL SERVICIO"**.

Entre la fecha en que **"EL ADMINISTRADOR DEL CONTRATO"** notifica a **"EL PROVEEDOR"** el incumplimiento en la prestación de **"EL SERVICIO"** y aquella en que **"EL PROVEEDOR"** realice la corrección del mismo y hasta en tanto ello no se cumpla, **"EL SERVICIO"** no se tendrá por recibido o aceptado a satisfacción.

DÉCIMA TERCERA.- MODIFICACIONES DEL CONTRATO. En términos de lo establecido en el artículo 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, **"LA CEAV"** podrá dentro de su presupuesto aprobado y disponible, bajo su responsabilidad y por razones fundadas y explícitas, acordar con **"EL PROVEEDOR"** el incremento o decremento del monto del Contrato o la cantidad de **"EL SERVICIO"** solicitado, mediante modificaciones al mismo, siempre que éstas no rebasen, en conjunto, el 20% del monto o cantidad de los conceptos o volúmenes establecidos originalmente en el mismo y el precio sea igual al pactado inicialmente.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

Lo anterior, de conformidad con los supuestos previstos en los artículos 91, 92 y 98, último párrafo del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público,

Cualquier modificación al Contrato deberá formalizarse por escrito por parte de **"LA CEAV"**, el instrumento legal respectivo será suscrito por el/la servidor/a público/a que lo haya hecho en el Contrato o quien lo/la sustituya o supla o esté facultado/a para ello.

De conformidad con lo establecido en el artículo 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, no procederá cambio alguno que implique otorgar condiciones más ventajosas a **"EL PROVEEDOR"** respecto de las establecidas originalmente.

Con fundamento en el artículo 91 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, por caso fortuito o fuerza mayor o por causas atribuibles a **"LA CEAV"**, esta última podrá modificar el presente Contrato a efecto de prorrogar el plazo para la prestación de **"EL SERVICIO"**. En este supuesto deberá formalizarse el convenio modificatorio respectivo, sin que proceda la aplicación de penas convencionales por atraso.

La modificación del plazo por caso fortuito o fuerza mayor, podrá ser solicitada por **"EL PROVEEDOR"** o por **"LA CEAV"**.

El escrito en el que se señale el caso fortuito o fuerza mayor, deberá ser presentado ante **"EL ADMINISTRADOR DEL CONTRATO"**, debidamente firmado por **"EL PROVEEDOR"**, dentro de los 5 días naturales posteriores al evento que le impida el cumplimiento de las obligaciones contraídas, así como anexar la constancia de dichos hechos.

En caso de que **"EL PROVEEDOR"** no obtenga la prórroga de referencia por ser causa imputable a éste el atraso, se hará acreedor a la aplicación de penas convencionales.

DÉCIMA CUARTA.- PENAS CONVENCIONALES. Las penas convencionales por atraso en la prestación de **"EL SERVICIO"** que se aplicarán a **"EL PROVEEDOR"**, serán de acuerdo con lo establecido en el artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 95 y 96 de su Reglamento y conforme a lo estipulado en el presente Contrato y su **Anexo I**, en los términos siguientes:



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

No.	Motivo	Nivel de Servicio	Valor de aplicación (VA)	Frecuencia	Referencia
1	Atraso en la entrega de acta de la recepción y memoria técnica del servicio.	5 días hábiles después de la finalización de cada sitio migrado.	0.05%, sobre el valor total de la facturación del mes, antes de I.V.A.	Por cada día natural de atraso.	Numeral 6 del Anexo I (Entregables iniciales)
2	Atraso en la entrega de reportes mensuales	Dentro de los primeros 5 días hábiles de cada mes.	0.05%, sobre el valor total de la facturación del mes, antes de I.V.A.	Por cada día natural de atraso.	Numeral 6 del Anexo I (Entregables mensuales)
3	Atraso en la entrega, instalación y configuración del equipamiento.	Un día natural previo al inicio del servicio (19 de diciembre del 2019).	5%, sobre el valor mensual del equipo no entregado, instalado y configurado.	Por cada día natural de atraso.	Numeral 7.1.1 del Anexo I (Entrega, Instalación y configuración)
4	Atraso en la Configuración, de las herramientas de gestión, monitoreo y administración.	30 días naturales después de la fecha de inicio del servicio (19 de diciembre del 2019).	5%, sobre el valor mensual de la herramienta no configurada.	Por cada día natural de atraso.	Numeral 7.1.1 del Anexo I (Entrega, Instalación y configuración)
5	Atraso en la entrega de servicio del cambio de domicilio.	30 días naturales de la solicitud oficial.	5%, sobre el valor total de la facturación del mes, antes de I.V.A.	Por cada día natural de atraso.	Numeral 3.6.1. del Anexo I (Cambios de Domicilio)
6	Atraso en la entrega de equipo adicional.	30 días naturales de la solicitud oficial	5%, sobre el valor total de la facturación del mes, antes de I.V.A.	Por cada día natural de atraso.	Numeral 3.6.2 del Anexo I (Equipo adicional)
7	Atraso en la migración del equipamiento.	45 días naturales después de la fecha de inicio del servicio.	5%, sobre el valor mensual del equipo no migrado.	Por cada día natural de atraso.	Numeral 7.1.2 del Anexo I (Migración)

Para el pago de las penas convencionales, "LA CEAV", a través de "EL ADMINISTRADOR DEL CONTRATO", informará por escrito a "EL PROVEEDOR"



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA

el cálculo de la pena correspondiente indicando el tiempo de atraso, así como la base para su cálculo y el monto de la pena a que se haya hecho acreedor.

"LA CEAV" a través de **"EL ADMINISTRADOR DEL CONTRATO"** notificará a **"EL PROVEEDOR"** vía oficio el cálculo de la pena correspondiente indicando el tiempo de atraso, así como la base para su cálculo y el monto de la pena a que se haya hecho acreedor, para que en un plazo que no exceda de cinco días hábiles contados a partir de dicha notificación, realice el pago mediante el formato e5cinco del Sistema de Administración Tributaria (cerrando a pesos el monto que contenga cantidades de 1 a 50 centavos ajustándolo a la unidad inmediata inferior y los que contengan 51 a 99 centavos a la inmediata superior). En caso de que **"EL PROVEEDOR"** no realice el pago solicitado dentro del plazo establecido, **"LA CEAV"** no procederá a realizar el pago del comprobante fiscal digital correspondiente.

DÉCIMA QUINTA.- DEDUCCIONES. Las deducciones por incumplimiento parcial o deficiente en la prestación de **"EL SERVICIO"** que se aplicarán a **"EL PROVEEDOR"**, serán de acuerdo con lo establecido en el artículo 53 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 97 de su Reglamento y conforme a lo estipulado en el presente Contrato y su **Anexo I**, en los siguientes casos:

No.	Motivo	Valor de aplicación (VA)	Frecuencia	Referencia
1	Incumplimiento parcial o deficiente en la entrega de reportes.	0.05% del valor total de la facturación del mes en que se presentó el incumplimiento antes del IVA por cada reporte que caiga en este supuesto.	Por cada día natural hasta que se subsane la deficiencia.	Numeral 6 del Anexo I (Entregables)
2	Incumplimiento parcial o deficiente en la entrega, instalación y configuración del equipamiento.	5% del valor total de la facturación del mes en que se presentó el incumplimiento antes del IVA.	Por cada día natural hasta que se subsane la deficiencia.	Numeral 7.1.1 del Anexo I (Entrega, instalación y configuración)
3	Incumplimiento parcial o deficiente en la atención y solución de incidentes	0.05% del valor total de la facturación del mes en que se presentó el incumplimiento antes del IVA por cada reporte que caiga en este supuesto.	Por cada día natural hasta que se subsane la deficiencia.	Numeral 4 del Anexo I (Niveles de Servicio)



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

4	Incumplimiento parcial o deficiencia en las herramientas de gestión, monitoreo y administración.	0.1% del valor total de la facturación del mes en que se presentó el incumplimiento antes del IVA.	Por cada día natural hasta que se subsane la deficiencia.	Numeral 7.1.1 del Anexo I (Entrega, instalación y configuración)
5	Incumplimiento parcial o deficiencia en el cambio de domicilio.	0.5% del valor total de la facturación del mes en que se presentó el incumplimiento antes del I.V.A.	Por cada día natural hasta que se subsane la deficiencia.	Numeral 3.6.1 del Anexo I (Cambios de domicilio)
6	Incumplimiento parcial o deficiencia en la entrega de equipo adicional.	5% del valor total de la facturación del mes en que se presentó el incumplimiento antes del I.V.A.	Por cada día natural hasta que se subsane la deficiencia.	Numeral 3.6.2 del Anexo I (Equipo adicional)
7	Incumplimiento parcial o deficiencia en la disponibilidad mensual del equipo Switch Core, Firewall UTM Tipo A y B, Teléfonos IP Básicos, Semi Ejecutivo, Secretarial, Call Center, Basada en Software, Terminal Audio Conferencia y Gateway Central, así como Remoto y Sistemas de Administrador de Llamadas, Telefonía IP, Call Center, Grabación y Tarificación Sea menor a 99.50%.	Después de 219 minutos de caída mensual se aplicará una deductiva del 1% sobre el monto mensual del equipo y/o servicio deficiente y por cada periodo equivalente posterior, se aplicará la misma deductiva.	Después de 219 minutos de caída mensual se aplicará una deductiva del 1% sobre el monto mensual del equipo y/o servicio deficiente y por cada periodo equivalente se aplicará la misma deductiva.	Numeral 4 del Anexo I (Niveles de servicio)



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA

8	Incumplimiento parcial o deficiencia en la disponibilidad mensual del equipo Switches de Acceso Tipo A y B, Controlador de Wireless y Puntos de Acceso sea menor a 99.20%.	Después de 350 minutos de caída mensual se aplicará una deductiva del 1% sobre el monto mensual del equipo y/o servicio deficiente y por cada periodo equivalente posterior se aplicará la misma deductiva,	Después de 350 minutos de caída mensual se aplicará una deductiva del 1% sobre el monto mensual del equipo y/o servicio deficiente y por cada periodo equivalente posterior se aplicará la misma deductiva.	Numeral 4 del Anexo I (Niveles de servicio)
9	Incumplimiento parcial o deficiencia en la disponibilidad mensual de la Consolas de Monitoreo y Operadora sea menor a 99.00%.	Después de 436 minutos de caída mensual se aplicará una deductiva del 1% sobre el monto mensual del equipo y/ o servicio deficiente y por cada periodo equivalente posterior se aplicará la misma deductiva,	Después de 436 minutos de caída mensual se aplicará una deductiva del 1% sobre el monto mensual del equipo y/o servicio deficiente y por cada periodo equivalente posterior se aplicará la misma deductiva.	Numeral 4 del Anexo I (Niveles de servicio)

Para aplicar las deducciones, "LA CEAV" a través de "EL ADMINISTRADOR DEL CONTRATO", notificará a "EL PROVEEDOR" el monto de las mismas para que éste presente su comprobante fiscal digital y la nota de crédito por el monto a deducir (cerrando a pesos el monto que contenga cantidades de 1 a 50 centavos ajustándolo a la unidad inmediata inferior y los que contengan de 51 a 99 centavos a la inmediata superior).

La acumulación de las deducciones, no excederá del importe de la garantía de cumplimiento del monto máximo del presente Contrato, sin considerar el I.V.A., en cuyo caso, se procederá al inicio del procedimiento de rescisión del Contrato.

DÉCIMA SEXTA.- RESCISIÓN ADMINISTRATIVA DEL CONTRATO. "LAS PARTES" convienen en que "LA CEAV" podrá, sin responsabilidad alguna, rescindir administrativamente en cualquier momento este Contrato. Dicha rescisión operará de pleno derecho, sin necesidad de intervención judicial.

Las causas que pueden dar lugar a la rescisión administrativa del Contrato por parte de "LA CEAV", son las siguientes:



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA

1. Por no apegarse a lo estipulado en el Contrato.
2. Cuando **"EL PROVEEDOR"** no cumpla con cualquiera de las especificaciones, características de **"EL SERVICIO"**, plazos para la entrega del mismo, las condiciones establecidas en este Contrato y en su **Anexo I**, así como con las contenidas en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y su Reglamento y demás disposiciones administrativas sobre la materia.
3. Si **"EL PROVEEDOR"** es declarado en concurso mercantil en los términos de la Ley de Concursos Mercantiles, o cualquier circunstancia análoga que afecte su patrimonio en tal forma que le impida cumplir con las obligaciones asumidas en el Contrato.
4. Por no entregar **"EL PROVEEDOR"** la garantía de cumplimiento solicitada en este Contrato o entregarla fuera del plazo establecido.
5. Por resolución de autoridad competente que impida a **"EL PROVEEDOR"** el cumplimiento de las obligaciones contraídas.
6. Cuando se agote el monto máximo de la garantía de cumplimiento, contabilizando para ello, el importe de las penas convencionales y/o deducciones a las que **"EL PROVEEDOR"** se haya hecho acreedor.
7. Por presentar la garantía de cumplimiento apócrifa.
8. Por negarse a reponer **"EL SERVICIO"** rechazado por **"LA CEAV"**.
9. Por negar a **"LA CEAV"** o a quienes estén facultados por ella, las facilidades para la supervisión en la prestación de **"EL SERVICIO"**.
10. Si se comprueba que alguna de las manifestaciones realizadas por **"EL PROVEEDOR"**, se realizó con falsedad.
11. Por contravenir los términos y condiciones del Contrato o las disposiciones de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento y los demás ordenamientos legales que resulten aplicables.
12. En general, por cualquier otra causa imputable a **"EL PROVEEDOR"**.

"LA CEAV" llevará a cabo dicho procedimiento de rescisión, de conformidad con los artículos 54 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 98 de su Reglamento.

De conformidad con el artículo 99 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, concluido el procedimiento de rescisión, se formulará y notificará el finiquito correspondiente, dentro de los 20 días naturales siguientes a la fecha en que se comunique la rescisión, debiéndose indicar los pagos que deban efectuarse y demás circunstancias del caso.

DÉCIMA SÉPTIMA.- TRANSFERENCIA DE DERECHOS Y OBLIGACIONES. **"EL PROVEEDOR"** no podrá transferir total o parcialmente, a favor de cualquier otra persona física o moral, distinta a aquella a la que se le hubiere adjudicado el Contrato, los derechos y obligaciones derivados del mismo.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

Conforme al artículo 46, último párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, se exceptúa de lo anterior lo relacionado con los derechos de cobro, en cuyo caso se deberá contar con la conformidad previa y por escrito de **"LA CEAV"**, deslindándose la misma de toda responsabilidad por la decisión tomada.

DÉCIMA OCTAVA.- CADENAS PRODUCTIVAS. En virtud de que **"LA CEAV"** está incorporada al Programa de Cadenas Productivas de Nacional Financiera, S.N.C., Institución de Banca de Desarrollo, manifiesta su conformidad para que **"EL PROVEEDOR"** pueda ceder sus derechos de cobro a favor de un Intermediario Financiero que esté incorporado a la Cadena Productiva de **"LA CEAV"** mediante operaciones de Factoraje o Descuento Electrónico.

DÉCIMA NOVENA.- TERMINACIÓN ANTICIPADA. Con fundamento en los artículos 54 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 102 de su Reglamento, **"LA CEAV"** tendrá la facultad de dar por terminado anticipadamente este Contrato cuando concurren razones de interés general, o bien, cuando por causas justificadas se extinga la necesidad de requerir **"EL SERVICIO"** 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 emitida por la Secretaría de la Función Pública.

La terminación anticipada se sustentará mediante dictamen que precise las razones o las causas justificadas que den origen a la misma. **"LA CEAV"** previa petición y justificación de **"EL PROVEEDOR"**, reembolsará a éste los gastos no recuperables en que haya incurrido siempre que éstos sean razonables, estén debidamente comprobados y se relacionen directamente con el presente Contrato, los cuales estarán limitados, según corresponda, a los conceptos previstos en el artículo 102 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público. Para efectos de lo anterior, las partes deberán celebrar el convenio respectivo.

"EL PROVEEDOR" podrá solicitar a **"LA CEAV"** 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.

Los gastos no recuperables, serán pagados dentro de un término que no podrá exceder de 45 días naturales posteriores a la solicitud por escrito, mediante la cual **"EL PROVEEDOR"**, fundamente y motive el pago de dichos gastos no recuperables.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

VIGÉSIMA.- PATENTES, MARCAS Y DERECHOS DE AUTOR. "EL PROVEEDOR" será responsable por el uso de patentes, licencias, derechos de autor y marcas que pudieran corresponder a terceros sobre los procedimientos que utilice y que proporcione para cumplir con el objeto del presente Contrato. En caso de infringir dichos conceptos o incurrir en violaciones legales, **"EL PROVEEDOR"** se obliga a resarcir a **"LA CEAV"** cualquier gasto comprobable que ésta erogue por dichos conceptos o derivado de cualquier responsabilidad que le haya sido imputada por autoridad competente.

VIGÉSIMA PRIMERA.- RELACIONES LABORALES. "LA CEAV" y **"EL PROVEEDOR"** aceptan y reconocen expresamente que no son aplicables a este Contrato, las disposiciones de la Ley Federal del Trabajo, ni de la Ley Federal de los Trabajadores al Servicio del Estado, Reglamentaria del apartado "B" del artículo 123 Constitucional. **"LA CEAV"** no adquiere, ni reconoce obligación alguna de carácter laboral, a favor de **"EL PROVEEDOR"**, ni de su personal.

El personal que se ocupará, con motivo de la prestación de **"EL SERVICIO"** materia de este Contrato, estará bajo la responsabilidad directa de **"EL PROVEEDOR"** y, como consecuencia, en ningún momento se considerará a **"LA CEAV"** como patrón sustituto o solidario, ni a **"EL PROVEEDOR"** como intermediario sino como patrón en términos de lo previsto en el artículo 15-A de la Ley del Seguro Social.

Por lo anterior, **"LA CEAV"** no tendrá relación alguna de carácter laboral con dicho personal y, consecuentemente, queda liberada de cualquier responsabilidad, obligándose **"EL PROVEEDOR"** a responder a todas las reclamaciones que sus trabajadores presenten en su contra o en contra de **"LA CEAV"**, con relación a los ordenamientos en materia de trabajo, higiene y seguridad social.

VIGÉSIMA SEGUNDA.- SUSPENSIÓN DEL CONTRATO. En términos de lo establecido en el artículo 55 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 102 de su Reglamento, cuando en la prestación de **"EL SERVICIO"** se presente caso fortuito o de fuerza mayor, **"LA CEAV"**, bajo su responsabilidad, podrá suspender la prestación de **"EL SERVICIO"**, en cuyo caso únicamente se pagará aquel que hubiese sido efectivamente prestado, debiendo celebrar las partes, el convenio respectivo.

La suspensión de **"EL SERVICIO"** se sustentará mediante dictamen, el cual deberá ser elaborado por **"EL ADMINISTRADOR DEL CONTRATO"**, en el cual se precisen las razones o causas justificadas que den origen a la misma.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

Cuando la suspensión obedezca a causas imputables a **"LA CEAV"**, previa petición y justificación de **"EL PROVEEDOR"**, aquélla le reembolsará los gastos no recuperables que se originen durante el tiempo que dure la suspensión.

Dicho pago será procedente, cuando los mencionados gastos sean razonables, estén debidamente comprobados y se relacionen directamente con el presente Contrato, los cuales estarán limitados, según corresponda, a los conceptos previstos en el artículo 102 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

"LAS PARTES" pactarán el plazo de suspensión; si al término del mismo, no puede reiniciar **"EL SERVICIO"**, podrá iniciarse la terminación anticipada a que se hace referencia en la cláusula que antecede.

"EL PROVEEDOR" podrá solicitar a **"LA CEAV"** el pago de gastos no recuperables en un plazo máximo de un mes, contado a partir de la fecha de la suspensión del Contrato.

Los gastos no recuperables, serán pagados dentro de un término que no podrá exceder de 45 días naturales posteriores a la solicitud por escrito, mediante la cual **"EL PROVEEDOR"**, fundamente y motive el pago de dichos gastos no recuperables.

VIGÉSIMA TERCERA.- RESPONSABILIDAD OBJETIVA. **"EL PROVEEDOR"** responderá de los daños y perjuicios que por inobservancia y negligencia de su parte llegue a causar a **"LA CEAV"** y/o a terceros, así como de cualquier otra responsabilidad en que hubiera incurrido durante la prestación de **"EL SERVICIO"**, con excepción de los que hayan acontecido por caso fortuito o fuerza mayor, por lo que se obliga a responder por dichos conceptos quedando obligado a resarcir a **"LA CEAV"**, de cualquier gasto o costo que ésta erogue por dichos supuestos o pérdida causada.

VIGÉSIMA CUARTA.- CONFIDENCIALIDAD. **"EL PROVEEDOR"** y el personal contratado por éste para prestar **"EL SERVICIO"** objeto de este Contrato, deberán guardar absoluta confidencialidad de toda la información y documentación a la que, con motivo de la prestación de **"EL SERVICIO"** tengan acceso, de forma escrita u oral, así como aquella que se genere con motivo de la prestación del mismo, en el entendido de que en caso contrario se procederá conforme a derecho por los daños o perjuicios que causen a **"LA CEAV"** las revelaciones que se llegaren a realizar.

Lo anterior, sin perjuicio de las acciones que implemente **"LA CEAV"** por la manipulación, uso, falsificación, duplicado, reproducción, venta, publicación de la información y/o documentación a la que con motivo de la prestación de **"EL**



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

SERVICIO tengan acceso, así como, los daños a terceros o divulgación de documentación oficial federal y las penas que por tal motivo, sean impuestas a **"EL PROVEEDOR"**.

VIGÉSIMA QUINTA.- LEGISLACIÓN APLICABLE. En todo lo no previsto en este Contrato se estará a lo dispuesto en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y su Reglamento; y en lo no previsto por esta Ley, serán aplicables el Código Civil Federal, la Ley Federal de Procedimiento Administrativo, el Código Federal de Procedimientos Civiles, la Ley Federal de Presupuesto y Responsabilidad Hacendaria y su Reglamento.

VIGÉSIMA SEXTA.- NULIDAD PARCIAL. "LAS PARTES" acuerdan que si por cualquier motivo o circunstancia, parte del presente Contrato es declarado nulo por virtud de sentencia firme o por así establecerlo alguna disposición legal presente o futura, tal situación no invalidará en forma alguna la parte restante del mismo, debiendo entonces ser aplicada la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y su Reglamento, y de manera supletoria, el Código Civil Federal, la Ley Federal de Procedimiento Administrativo, el Código Federal de Procedimientos Civiles, así como los Tratados y Convenios Internacionales de los cuales México sea parte, y demás normatividad que resulte aplicable del derecho común, esto en concordancia y sin menoscabo del texto contractual cuya validez no fuere afectada.

No obstante lo anterior, para cualquier aspecto presupuestal que se derive del presente Contrato, deberá aplicarse la Ley Federal de Presupuesto y Responsabilidad Hacendaria, su Reglamento y normatividad conexas en la materia.

VIGÉSIMA SÉPTIMA.- CLÁUSULA DE CONCILIACIÓN. "LAS PARTES" acuerdan que para el caso de que se presenten desavenencias derivadas de la ejecución y cumplimiento del presente Contrato se someterán al procedimiento de conciliación establecido en los artículos 77, 78, 79 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y 126 al 136 de su Reglamento.

VIGÉSIMA OCTAVA.- SOLUCIÓN DE CONTROVERSIAS Y JURISDICCIÓN. "LAS PARTES" convienen en que, para la interpretación y cumplimiento de las obligaciones derivadas del presente Contrato, se someterán a la jurisdicción y competencia de los Tribunales Federales radicados en la Ciudad de México, renunciando **"EL PROVEEDOR"**, al fuero que por razón de su domicilio presente o futuro, le pudiera corresponder.

Leído que fue el presente Contrato y enteradas **"LAS PARTES"** de su contenido y alcance legal, lo firman, libre de vicios en el consentimiento, tales como error,



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA

dolo, mala fe o violencia, en tres tantos, en la Ciudad de México, el día 29 de noviembre de 2019.

POR "LA CEAV"

**DIRECCIÓN GENERAL DE
ADMINISTRACIÓN Y FINANZAS**

POR "EL PROVEEDOR"

**C. CRISTÓBAL ERNESTO GARCÍA VEGA
APODERADO LEGAL
ORBEN COMUNICACIONES, S.A.P.I. DE C.V.**

En suplencia por ausencia de la persona Titular de la Dirección General de Administración y Finanzas con fundamento en los artículos 5, fracción XI inciso c; 23 bis párrafo segundo y 34 fracción XVIII del Estatuto Orgánico de la Comisión Ejecutiva de Atención a Víctimas, última reforma publicada en el Diario Oficial de la Federación el 20 de diciembre de 2018, suscribe el presente Contrato el Director de Recursos Materiales y Servicios Generales, el C.P. Salvador Osogobio Villegas.

POR "EL ADMINISTRADOR DEL
CONTRATO"

**ING. ROGELIO MESTA ESTRADA
DIRECTOR DE TECNOLOGÍAS DE LA
INFORMACIÓN**

Las firmas que anteceden forman parte del Contrato número **CEAV-C-56-2019**, celebrado entre la **COMISIÓN EJECUTIVA DE ATENCIÓN A VÍCTIMAS** y **ORBEN COMUNICACIONES, S.A.P.I. DE C.V.**



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

Anexo I

TÉRMINOS DE REFERENCIA



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA

1. Objetivo de "EL SERVICIO"

Este servicio tiene como objetivo proveer a la Comisión Ejecutiva de Atención a Víctimas, en adelante "**LA CEAV**", de la infraestructura de comunicaciones (SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA) necesaria para ofrecer una mejor conectividad entre las diferentes oficinas de "**LA CEAV**" optimizando la transmisión de datos, así como incrementar la seguridad en todos los puntos de las comunicaciones de la red de "**LA CEAV**", a través de un servicio administrado de red de voz, datos y seguridad.

Objetivos específicos.

- 1) Proveer el equipamiento necesario para la prestación del servicio para "**LA CEAV**"; basado en un esquema de niveles de servicio;
- 2) Contar con una red de datos que optimice la velocidad de intercambio de información, logrando un flujo continuo de la misma y preparada para el crecimiento que demande a futuro los objetivos de "**LA CEAV**" y las nuevas tecnologías;
- 3) Sistema de voz para brindar servicios de comunicación, colaboración y movilidad que permitan una óptima interacción del personal;
- 4) Sistemas que garanticen la seguridad de la información de usuarios de "**LA CEAV**" que transmiten información hacia internet;
- 5) Lograr una operación continua mediante un servicio basado en el cumplimiento de niveles de servicio, actualización periódica de los sistemas, y monitoreo de la red; y
- 6) Respuestas oportunas a los requerimientos de la oficina central y centros de atención integral en los estados de "**LA CEAV**" a partir de servicios bajo demanda de los sistemas e infraestructura.

2. Vigencia de "EL SERVICIO"

La vigencia de la prestación de "**EL SERVICIO**" iniciará a las 00:00 horas del 20 de diciembre del 2019 y concluirá a las 23:59 horas del 30 de abril de 2020.

3. Características de "EL SERVICIO"

Los procesos y requerimientos a los cuales se refiere "**LA CEAV**" en este numeral son enunciativos más no limitativos.



CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

3.1 Generalidades

- a) **"LA CEAV"** cuenta con una oficina central, un anexo en la Ciudad de México y 32 Centros de Atención Integral (CAI), por lo que **"EL PROVEEDOR"** deberá de considerar la implementación en cada uno de ellos; así como los costos inherentes de transportación, envío y mantenimiento de la solución.

Así mismo **"LA CEAV"** podrá solicitar que el servicio se preste en nuevos sitios dentro del contrato.

- b) **"EL PROVEEDOR"** deberá considerar el cableado y los misceláneos compatibles necesarios para la conectividad entre los dispositivos de red y la conexión con los dispositivos terminales en caso de que el cableado existente no se encuentre en correcto estado físico y/o se requiera la agregación de servicio no existente en la red de **"LA CEAV"**.
- c) **"EL PROVEEDOR"** deberá considerar equipos de respaldo de energía (UPS) con una autonomía que permita soportar al menos 20 minutos de infraestructura de la red local, red amplia, seguridad perimetral y telefonía requerida por **"LA CEAV"** en el presente documento ante algún problema en la energía de cada uno de los sitios.
- d) La operación y funciones de **"LA CEAV"** requieren de una baja latencia en sus procesos sensibles y garantizar las transacciones sin errores a los nuevos servicios centrales. Además de garantizar el óptimo funcionamiento de la red incrementando la capacidad de conmutación y de tráfico para poder dar mejores tiempos de respuesta.
- e) **"LA CEAV"** requiere ser proactivo en la integración de funcionalidades demandadas por la operación, por lo que se busca mayor capacidad en la Red LAN y aplicativos que puedan ser desarrolladas por **"LA CEAV"**.
- f) **"LA CEAV"** requiere una red capaz de diferenciar a los usuarios de la red de acuerdo a su rol y poder aplicar políticas de calidad de servicio, permisión o negación de acceso a servicios específicos, mayor control de ancho de banda, esto con la finalidad de brindar mayor seguridad sobre la red e información confidencial de **"LA CEAV"** y optimizar el uso de los anchos de banda con los que se cuenta.
- g) **"LA CEAV"** requiere un servicio integral de comunicación de voz, con un procesamiento centralizado con la capacidad de brindar una solución distribuida permitiendo tener el control del sistema en el sitio central de **"LA CEAV"** y poder brindar servicios distribuidos mediante nodos a sus



CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

centros de atención integral estatales actuales y aquellas nuevas que resulten del crecimiento de **"LA CEAV"**.

- h) Es imperativo contar con una infraestructura (equipamiento de hardware y software) que garantice un ciclo de vida de la vigencia del contrato, con actualizaciones de software y con las refacciones necesarias para contar con una operación eficiente y un nivel de servicios de calidad acorde con las necesidades de los usuarios de **"LA CEAV"**.
- i) La infraestructura debe de ofrecer un esquema de crecimiento simple y ágil, lo cual permitirá a **"LA CEAV"** tener la flexibilidad necesaria para dotar de servicios de comunicación a los nuevos sitios o nuevas localidades.
- j) Contar con una base de datos unificada y en alta disponibilidad para toda la solución, lo cual permitirá que en caso de que alguno de los sitios remotos se apague (por fallas eléctricas) no se pierda la configuración de ese sitio en particular.
- k) La infraestructura que **"EL PROVEEDOR"** suministre a **"LA CEAV"** podrá estar o no estar asegurados, a criterio y decisión de **"EL PROVEEDOR"**. Sin embargo, en caso de daño, siniestro o robo, el equipo deberá reemplazarse. Los daños ocasionados por los usuarios en forma accidental o por el uso cotidiano también deberán ser cubiertos por **"EL PROVEEDOR"** y sin costo para **"LA CEAV"**.
- l) **"LA CEAV"** busca contar con soluciones de tecnologías de última generación como:
 - **Movilidad.** Se requiere una solución que permita contar con funcionalidades de movilidad, lo cual permitirá a los usuarios (que tienen esa necesidad) contar con sus servicios telefónicos corporativos a través de sus laptops, smartphone o tabletas electrónicas.
 - **Uso de video y colaboración.** Se requiere el uso de video y colaboración entre las diferentes localidades de la Entidad para evitar costos de traslado y hacer más eficiente la comunicación entre los usuarios de **"LA CEAV"**.
 - **Centro de contacto.** Se requiere un servicio de centro de contacto que permita a la Entidad ofrecer un solo punto de contacto hacia los usuarios finales.
- m) El equipo deberá ser funcional original de fábrica, en cualquiera de sus componentes que lo conforman, además de cumplir con las características solicitadas.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

3.2 Características técnicas mínimas y descripción de servicios

Esta sección contiene las características técnicas mínimas y descripción de los requerimientos mínimos solicitados por "LA CEAV".

3.2.1 Switch Core Sitio Central

Características Principales

Se solicita un chasis virtual que cuente con al menos dos (switches físicos). El chasis virtual deberá incluir redundancia en ventiladores y sistema operativo y deberá soportar fuentes redundantes N+1 en cada switch que lo compone. El procesamiento deberá poder ser manejado por cada uno de los elementos del chasis virtual.

Interfaces y Fuentes Requeridas

- Soporte de fuentes de poder AC en arreglo redundante en cada elemento del chasis virtual.
- Las fuentes de poder deberán ser internas en el chasis de la unidad.
- 60 puertos 1G/10G Base-

Rendimiento y capacidades

De arquitectura tipo chasis virtual (IFR), la arquitectura deberá soportar funcionalidades en capas 2, 3 y 4, al activarlas el desempeño del equipo no deberá afectar el desempeño del equipo.

Para el chasis virtual (IRF):

- Esta funcionalidad deberá virtualizar 2 o más switches físicos en todas las capas y no solamente en la capa 2 de manera que las 2 o más unidades físicas se conviertan en una sola unidad lógica. No se aceptan soluciones donde se virtualicen múltiples entidades lógicas en un mismo dispositivo físico.
- Cada equipo que conforme el chasis virtual deberá soportar 6 o más puertos de 40Gbps que se utilizarán para la interconexión del chasis virtual.
- Cada elemento deberá soportar un mínimo de 30 puertos RJ45 1G/10G.
- Incluir un mínimo de 6 slots QSFP+ o similar con soporte de transceivers de 40Gbps y soporte de direct attach cables (DACs) de cobre de 40G.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

La arquitectura propuesta deberá de contar con una capacidad de conmutación de al menos 2.56 Tbps (en un chasis virtual las capacidades de los elementos se suman) para garantizar el procesamiento adecuado de la información, aun cuando todas las interfaces estén transfiriendo paquetes a su máxima velocidad y así evitar el bloqueo de las mismas. Debido a que es un equipo de Backbone, este deberá de realizar un forwarding en capa 2 y capa 3 de al menos 1,200 Mpps, deberá soportar al menos un ancho de banda en la unidad de 480 Gbps agregado entre los elementos del chasis virtual (IRF) (conexión entre equipos físicos), el chasis virtual deberá de soportar al menos 256,000 direcciones MAC.

El chasis virtual deberá de soportar el estándar 802.1q, permitiendo tener al menos 4,094 VLANs para segmentar el tráfico de la red, se deberá de poder crear VLANs basadas en 802.1q.

Así mismo deberá de soportar VLAN Stacking, también conocidas como encapsulamiento Q-in-Q.

El equipo deberá de soportar los siguientes protocolos:

Protocolos de Multicast

- Internet Group Management Protocol (IGMP) v1/v2/v3 snooping.
- Protocol Independent Multicast – Sparse Mode (PIM-SM) ASM and SSM.
- Protocol Independent Multicast – Dense Mode (PIM-DM).
- Distance Vector Multicast Routing Protocol (DVMRP).
- Multicast Listener Discovery (MLD) v1/v2 snooping.

Administración y análisis de tráfico

- RMON, SNMP V1, V2 Y V3.
- SFLOW o NetFlow.
- SSH, HTTP y HTTPS.
- DHCP Relay.

Protocolos Capa 2

- IEEE 802.3ad (Agregación de enlaces).
- IEEE 802.1AX (Agregación de enlaces).
- IEEE 802.1s (Multiple Spanning Tree).
- IEEE 802.1Qbb (Priority Flow Control).
- IEEE 802.1Qbg Edge Virtual Bridging (EVB).
- IEEE 802.1Qaz Enhanced Transmission Selection (ETS).



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- IEEE 802.1Qaz Data Center Bridging Capabilities Exchange Protocol (DCBX).
- IEEE 802.1Qbg Edge Virtual Bridging (EVB).
- IEEE 802.1aq Shortest Path Bridging (SPB-M).
- IEEE 802.1s (Multiple Spanning Tree).
- RFC 1765 OSPF Database Overflow.
- RFC 1850/2328 OSPF v2 and MIB.
- RFC 2154 OSPF MD5 Signature.
- RFC 2370/3630 OSPF Opaque LSA.
- RFC 3101 OSPF NSSA Option.
- RFC 3623 OSPF Graceful Restart.
- RFC 2740 OSPFv3 for IPv6.

Protocolos de Ruteo IPv6

- Multiple Virtual Routing and Forwarding (VRF).
- Internet Control Message Protocol version 6 (ICMPv6).
- Static routing.
- Routing Information Protocol Next Generation (RIPng).
- Open Shortest Path First (OSPF) v3 with Graceful Restart.
- Intermediate System to Intermediate System (IS-IS) with graceful restart.
- Soporte de ruteo IS-IS.
- BGP v4 multiprotocol extensions for IPv6 routing (MP-BGP).
- Graceful Restart extensions for OSPF and BGP.
- Virtual Router Redundancy Protocol (VRRPv3).
- Neighbor Discovery Protocol (NDP).
- Policy-based routing and server load balancing.

Estándares de BGP

- RFC 1269/1657/4273 BGP v3 and v4 MIB.
- RFC 1403/1745 BGP/OSPF Interaction.
- RFC 1771-1774/2842/2918/3392/4271 BGP v4.
- RFC 1965 BGP AS Confederations.
- RFC 1966 BGP Route Reflection.
- RFC 1997/1998/4360 BGP Communities Attribute.
- RFC 2042/5396 BGP New Attribute.
- RFC 2385 BGP MD5 Signature.
- RFC 2439 BGP Route Flap Damping.
- RFC 2545 BGP-4 Multiprotocol Extensions for IPv6 Routing.
- RFC 2858/4760 Multiprotocol Extensions for BGP-4.
- RFC 3065 BGP AS Confederations.



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- RFC 4456 BGP Route Reflection.
- RFC 4486 Subcodes for BGP Cease Notification.
- RFC 4724 - Graceful Restart for BGP.
- RFC 5492/5668/6793 BGP 4-Octet ASN.

Estándares de IS-IS

- RFC 1142/1195/3719/3787/5308 IS-IS v4.
- RFC 2763/2966/3567/3373 Adjacencies and route management.
- RFC 5120 M-ISIS: Multi Topology IS-IS.
- RFC 5306 Graceful Restart.
- RFC 5309/draft-ietf-isis-igp-p2p-over-lan Point to point over LAN.
- RFC 6329 IS-IS Extensions Supporting IEEE 802.1aq SPB.

Interfaces Soportadas.

- Puertos 1000Base-T/10G Base-T/10G Base-T
- Puertos 40G QSPF+.

Requerimientos Especiales:

- 1) Todos los interfaces deberán ser 100% Non-Blocking.
- 2) Deberá contar con tecnología que permita identificar, clasificar y seguir el movimiento de máquinas virtuales (VM) a través de la red de manera automática y manual. Indicar el nombre y funcionamiento de la tecnología ofertada.
- 3) Deberá contar con la capacidad de utilizar múltiples enlaces a diferentes equipos de manera simultánea sin depender de un solo árbol de STP para lo cual deberá contar con 802.1aq (SPB).
- 4) Debe incluir instalado y operativo soporte de Openflow 1.3 de forma que se pueda integrar a controladores SDN de terceros o propietarios del fabricante y tener la capacidad de agregar servicios en la red siguiendo la arquitectura de red SDN (Aplicación + Controlador SDN + Forwarding de paquetes).
- 5) Deberá contar con la capacidad de trabajar los siguientes protocolos estándares para Data Center: DCB (Data Center Bridging), PFC (Priority Flow Control - 802.1Qbb), Congestion Notification (802.1Qau), ETS (Enhanced Transmission Selection - 802.1Qaz), EVB (Edge Virtual Bridge - 802.1Qbg).
- 6) Deberá tener la capacidad de autoaprovisionamiento, donde sin intervención de un administrador de red, al interconectarse con otros equipos similares pueda automáticamente configurar una red con enlaces SPB, y pueda crear automáticamente una serie de VLANs para tal fin.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

3.2.2 Switches de Acceso tipo A de 48 puertos

Se solicita un equipo apilable de al menos 1 unidad de rack de altura. El equipo deberá de soportar redundancia en fuentes de poder y sistema operativo.

Rendimiento y capacidades

El equipo propuesto deberá de contar con una capacidad de conmutación de al menos 170 Gbps para garantizar el procesamiento adecuado de la información, aun cuando todas las interfaces estén transfiriendo paquetes a su máxima velocidad y así evitar el bloqueo de las mismas. Debido a que es un equipo de acceso, este deberá de realizar un forwarding en capa 2 de 130mpps. Respecto a las direcciones MAC, el equipo deberá de soportar al menos 16 mil.

El equipo deberá de soportar el estándar 802.1q, permitiendo tener al menos 4,094 VLANs para segmentar el tráfico de la red, se deberá de poder crear VLANs basadas en 802.1q.

Así mismo deberá de soportar VLAN Stacking, también conocidas como encapsulamiento de VLANs Q-in-Q.

El equipo deberá de soportar los siguientes protocolos:

- Ethernet IEEE 802.3, 10 Base-T.
- Fast Ethernet IEEE 802.3u, 100Base-TX.
- Gigabit Ethernet IEEE 802.3z, 802.3ab, 1000Base-T.
- 10Gigabit Ethernet IEEE 802.3ae.
- Soporte de interfaces 1000Base-SX, 1000Base-LX, 1000Base-LH, 10G-Base-SR, 10G-Base-LR.
- IEEE 802.1D, Spanning Tree Protocol.
- IEEE 802.1P QoS.
- IEEE 802.1Q VLAN Tagging.
- IEEE 802.1x.
- IEEE 802.1ag Ethernet CFM.
- IEEE 802.1AB LLDP.
- IEEE 802.1s MSTP.
- IEEE 802.1w RRSTP.
- IEEE 802.3ad Link aggregation.
- IEEE 802.3x.
- IEEE 802.3af PoE.
- IEEE 802.3at PoE+.
- Filtrado Multicast de Capa 2 y Capa 3.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Soporte de IGMPv2, IGMPv3 Snooping en IPv4 y MLD en IPv6 instalados y operativos.
- Capacidad instalada de VRRP o HSRP.
- Administración por interface de línea de comandos, SNMPv3 vía Software e interface web con ssl.
- Capacidad instalada de sFlow o NetFlow.
- Soporte de múltiples niveles de privilegios de acceso por consola para los administradores ya sea local o remotamente por SSH v2. Los equipos deben soportar un mínimo de 6 (seis) niveles.
- Herramienta de gestión WEB con capacidad de realizar todas las tareas de administración CLI.
- Soporte de IEEE 802.1x múltiples hosts y múltiples vlans por puerto.
- Soporte de ACLs por puerto, basados en información de Capas 2, 3 y 4.
- Soporte de port Mirror.
- Soporte de más de 1000 entradas en el ACL.
- Mecanismos de detección y cancelación de ataques del tipo DoS.
- Funcionalidad de QoS Multilayer. Clasificación de tráfico basada en direcciones MAC de origen y destino (Capa 2), direcciones IP de origen y destino (Capa 3) y puertos TCP/UDP (Capa 4).
- 8 colas de priorización por puerto.
- Soporte de al menos 4,000 VLAN ID según el estándar 802.1Q y 16K MAC address como mínimo.

Interfaces Soportadas

El equipo propuesto deberá de soportar por lo menos la siguiente cantidad de Interfaces, 48 puertos 10/100/1000BaseT, 2 puertos 1G/10G Full Duplex de fibra uplink y 2 puertos de stacking con una capacidad agregada de 40Gbps.

Funcionalidades

Capacidad de Stack con al menos 10Gbps por cada canal.

3.2.3 Switches de Acceso tipo B de 24 puertos

Se solicita un equipo apilable de al menos 1 unidad de rack de altura. El equipo deberá de soportar redundancia en fuentes de poder y sistema operativo.

Rendimiento y capacidades

El equipo propuesto deberá de contar con una capacidad de conmutación de al menos 128 Gbps para garantizar el procesamiento adecuado de la información, aun cuando todas las interfaces estén transfiriendo paquetes a su máxima



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

velocidad y así evitar el bloqueo de estas. Debido a que es un equipo de acceso, este deberá de realizar un forwarding en capa 2 de 95 mpps. Respecto a las direcciones MAC, el equipo deberá de soportar al menos 16,000 entradas.

El equipo deberá de soportar el estándar 802.1q, permitiendo tener al menos 4,094 VLANs para segmentar el tráfico de la red, se deberá de poder crear VLANs basadas en 802.1q.

Así mismo deberá de soportar VLAN Stacking, también conocidas como encapsulamiento de VLANs Q-in-Q.

El equipo deberá de soportar los siguientes protocolos:

- Ethernet IEEE 802.3, 10 Base-T.
- Fast Ethernet IEEE 802.3u, 100Base-TX.
- Gigabit Ethernet IEEE 802.3z, 802.3ab, 1000Base-T.
- 10Gigabit Ethernet IEEE 802.3ae.
- Soporte de interfaces 1000Base-SX, 1000Base-LX, 1000Base-LH, 10G-Base-SR, 10G-Base-LR.
- IEEE 802.1D, Spanning Tree Protocol.
- IEEE 802.1P QoS.
- IEEE 802.1Q VLAN Tagging.
- IEEE 802.1x.
- IEEE 802.1ag Ethernet CFM.
- IEEE 802.1AB LLDP.
- IEEE 802.1s MSTP.
- IEEE 802.1w RRSTP.
- IEEE 802.3ad Link Aggregation.
- IEEE 802.3x.
- IEEE 802.3af PoE.
- IEEE 802.3at PoE+.
- Filtrado Multicast de Capa 2 y Capa 3.
- Soporte de IGMPv2, IGMPv3 Snooping en IPv4 y MLD en IPv6 instalados y operativos.
- Capacidad instalada de VRRP o HSRP.
- Administración por Interface de línea de comandos, SNMPv3 vía Software e interface web con SSL.
- Capacidad instalada de sFlow o NetFlow.
- Soporte de múltiples niveles de privilegios de acceso por consola para los administradores ya sea local o remotamente por SSH v2. Los equipos deben soportar un mínimo de 6 (seis) niveles.
- Herramienta de gestión WEB con capacidad de realizar todas las tareas de administración CLI.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Soporte de IEEE 802.1x múltiples hosts y múltiples VLANs por puerto.
- Soporte de ACLs por puerto, basados en información de Capas 2, 3 y 4.
- Soporte de port Mirror.
- Soporte de más de 1000 entradas en el ACL.
- Mecanismos de detección y cancelación de ataques del tipo DoS.
- Funcionalidad de QoS Multi-Layer. Clasificación de tráfico basada en direcciones MAC de origen y destino (Capa 2), direcciones IP de origen y destino (Capa 3) y puertos TCP/UDP (Capa 4).
- 8 colas de priorización por puerto.
- Soporte de al menos 4,000 VLAN ID según el estándar 802.1Q y 16K MAC address como mínimo.

Interfaces Soportadas

El equipo propuesto deberá de soportar por lo menos la siguiente cantidad de interfaces, 24 puertos 10/100/1000BaseT, 2 puertos 1G/10G de fibra uplink y 2 puertos de stacking con una capacidad agregada de 40Gbps.

Funcionalidades

Capacidad de Stack con al menos 10Gbps por cada canal.

Perfilamiento LAN

Los switches de acceso Tipo A y Tipo B deberán tener la capacidad instalada ya sea con recursos propios o con recursos externos de poder controlar el acceso a la red y asignar perfiles de red o roles basándose en la identidad de los usuarios en el Directorio Activo haciendo uso del estándar 802.1x para las estaciones corporativas y de un portal web con soporte de SSL para los invitados cumpliendo con las siguientes características técnicas:

Capacidad de clasificar a cada usuario o dispositivo que requiera conexión a la red en un PERFIL o ROL, este perfil o rol deberá permitir asociarlo a una VLAN determinada y aplicarle un conjunto de políticas de acceso tipo firewall o ACL de capa 2, 3 y 4.

Los puertos deberán autenticar y segmentar a cada uno de los usuarios y dispositivos conectados a estos de manera independiente y dinámica cumpliendo con los siguientes requisitos:

Capacidad instalada de 802.1x múltiples clientes y múltiples VLANs en el mismo puerto de forma que todos los dispositivos que se conecten detrás de un puerto pasen por un proceso de autenticación 802.1x y cada una de estas



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

“SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA”

autenticaciones pueda ser manejada de manera independiente. No se aceptan soluciones donde la última autenticación reemplaza a las anteriores.

Si para clasificar a los usuarios y dispositivos en Perfiles o Roles se requiere de hardware y/o software adicional este debe agregarse de manera que pueda cubrir el 100% de los puertos ofertados y bajo una modalidad redundante. **“EL PROVEEDOR”** deberá incluir en su oferta todo lo que esta solución requiera incluyendo servidores, licencias y software.

Capacidad instalada de un Captive Portal para todos los puertos ofertados que ayude en el manejo de BYOD, de forma que los usuarios o dispositivos invitados puedan ser redireccionados automáticamente a este Captive Portal y puedan pasar por un proceso de autenticación. Se permitirá cumplir con este punto con un portal cautivo externo bajo una modalidad redundante.

3.3 Red inalámbrica de área local (WLAN).

Se requiere de un Sistema de Red inalámbrica para red de Área Local WLAN (Wireless Local Area Network), conformada bajo la arquitectura centralizada con dos switches/controladores centrales y puntos de acceso inalámbricos, para usarse como unidades remotas administrados por el controlador.

El sistema deberá proveer conectividad inalámbrica para múltiples usuarios y dispositivos como PDA inalámbricos, cámaras de vigilancia, computadores portátiles, teléfonos IP inalámbricos o IP softphones instalados en computadores portátiles, etc.

La solución de red inalámbrica solicitada debe contar con los más altos niveles de seguridad que involucrarán como mínimo las funcionalidades de Firewall, wireless Intrusion Protection, RF Spectrum Analysis así como el manejo de los más altos niveles de encriptación y autenticación con 802.1x + WPA2 + AES así como 802.1x + WPA + TKIP para los usuarios corporativos y Portal Web para los invitados.

La solución propuesta deberá trabajar bajo una arquitectura de controlador centralizado Real o Virtual el cual podrá ser del tipo appliance o virtualizado, la solución deberá permitir clasificar a todos los usuarios y dispositivos que requieran conexión a la red WiFi para lo cual se requiere que cada usuario o dispositivo que se conecte pueda ser clasificado en perfiles o roles que permitan una fácil y segura gestión de la red permitiendo asociar a cada perfil una VLAN, permisos de firewall y QoS.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

Se aceptarán soluciones que para lograr este objetivo requieran de hardware y/o software o licencias adicionales siempre y cuando se incluya todo lo necesario en su oferta.

De acuerdo a la densidad de Puntos de acceso requeridos y los niveles de crecimiento de la solución se ha definido que cada uno de los 2 controladores físicos o virtualizados requeridos cuente con una capacidad máxima de poder manejar hasta 128 Puntos de Acceso los cuales deberán estar 100% licenciados a nivel de AP, Firewall y Wireless Intrusion Protection.

La solución inalámbrica propuesta debe ser altamente escalable y de alto rendimiento pudiendo integrar centenares de usuarios y/o dispositivos conforme las necesidades de la red en cuanto a crecimiento.

La red inalámbrica propuesta deberá ser interoperable y compatible con la estructura de red propuesta, así como con los principales estándares internacionales y arquitecturas de red del mercado. El controlador administrará las funciones de los AP.

3.3.1 Controlador Wireless

- Cada controlador debe tener una capacidad instalada y licenciada de controlar 128 AP's como mínimo.
- Debe contar con un puerto de consola del tipo RJ-45.
- Debe manejar los estándares 802.11 a/b/g/n/ac.
- Debe permitir la implementación del Standard 802.1x sin necesidad de configurar un cliente en el Radius server cada vez que se instale un nuevo Access Point, solo se requerirá inscribir en el Radius Server al controlador (real o virtual) inalámbrico.
- Debe tener la capacidad instalada de Detección de Intrusos (IDS) o Wireless Intrusion Protection para redes 802.11 licenciada para todos los APs soportados por cada controladora, se aceptarán soluciones que para cumplir con este requerimiento requieran agregar hardware o/y software adicional siempre y cuando se entregue una solución de Detección de Intrusos para cada edificio contemplado para este proyecto.
- Debe tener la capacidad instalada de Firewall con cobertura para los 128 o más AP's.
- Debe poder aplicar políticas de acceso (Firewall) en función de la autenticación al Directorio Activo.
- Debe permitir la asignación de roles en función de la autenticación, estos roles permitirán asignar políticas de firewall y asignación de VLAN en función de la autenticación.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA

- Debe permitir aplicar control de ancho de banda por usuario de manera dinámica basándose en la autenticación del usuario, o al SSID que se conecta o al perfil o rol al que pertenezca.
- Debe poder identificar los sistemas operativos de los dispositivos que se conectan a la red.
- Deberá contar con tecnología que permita el balanceo de usuarios entre APs considerando no solamente las condiciones de ruido e interferencia de los APs si no que pueda tener visibilidad de las condiciones de los dispositivos conectados. Nombrar, detallar y documentar esta funcionalidad.
- Debe soportar los siguientes métodos de autenticación: 802.1x, MAC, Portal Web. Para lograr alcanzar todos estos métodos de autenticación se aceptará que los postores incluyan componentes de software y/o hardware adicionales a los controladores siempre y cuando sean del mismo fabricante.
- Debe contar con tecnología para el control dinámico de la RF y reaccionar automáticamente ante eventos de ruido e interferencia.
- Debe contar con una herramienta gráfica de planificación y diseño centralizada que controle a todos los controladores ofrecidos en el presente proyecto. Esta herramienta deberá poder monitorear las redes inalámbricas, armar mapas de calor y propagación de las señales, ubicación de los dispositivos conectados a la red inalámbrica, monitorear el tráfico de los dispositivos conectados a la red inalámbrica, detectar ataques en el aire como mínimo.
- Debe contar con una herramienta de gestión web embebida que permita flexibilidad y continuidad de operaciones.
- Debe asegurar Fast Roaming con un tiempo de paso de un AP a otro de no más de 50ms.
- Debe soportar tuneleo entre los AP's y el Controlador.
- Debe permitir la autocorrección ante la caída de un AP de forma que los más cercanos modifiquen su potencia para cubrir la pérdida de señal.

3.3.2 Puntos de Acceso

- Debe contar con dos Radios como mínimo y desarrollar una velocidad mínima de 300Mbps en 2.4Ghz y 300 Mbps en la banda de 5Ghz de manera simultánea.
- Deberá contar con 2 puertos 100/1000Base-TX como mínimo.
- Debe contar con un puerto de consola del tipo RJ-45.
- Debe trabajar bajo el protocolo 802.11 a/n y b/g/n/ac. (en simultáneo).
- Frecuencia de operación 2.4 Ghz y 5.7 Ghz. (en simultáneo).
- Soporte mínimo de 3x3 MIMO con un ancho de banda agregado de 1.8 Gbps sumando la capacidad de Ambos radios (2.4 GHz y 5GHz).



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Soporte de PoE 802.3af y 802.3at.
- Se aceptarán soluciones con antenas integradas y/o externas.
- Las antenas deben ser omnidireccionales con una ganancia de entre 3 a 4.5 dBi como mínimo.
- Deberá permitir la implementación de la tecnología que permita el balanceo de usuarios entre APs considerando no solamente las condiciones de ruido e interferencia de los APs si no que pueda tener visibilidad de las condiciones de los dispositivos conectados. Nombrar, detallar y documentar esta funcionalidad.
- Deben ser Access Points para uso Interno.
- Deben soportar una temperatura de trabajo de entre 0 y 50 Grados centígrados. Certificaciones.
 - Wi-Fi certified 802.11a/b/g/n/ac.
- Tasas de Transferencia soportadas.
 - En la banda definida para 802.11b/g: 1, 2, 5.5, 11.
 - En la banda definida para 802.11a: 6, 9, 12, 18, 24, 36, 48 y 54Mbps.
 - En las bandas definidas para 802.11n: hasta 600Mbps.
 - En las bandas de 5GHz para 802.11ac: hasta G6ps.
- Canales de operación.
- Para la frecuencia de 5GHz: Todos los canales comprendidos desde los 4920 MHz hasta los 5825 MHz.
- Para la frecuencia de 2.4GHz: Canales del 1 al 13 (en la banda de los 2412-2472. MHz)
- Métodos de Modulación.
 - 802.11b: BPSK, QPSK, CCK.
 - 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM.

3.3.3 Servicios de Seguridad

"EL PROVEEDOR" deberá suministrar la infraestructura necesaria para brindar servicios de Seguridad UTM en una modalidad de servicios administrados, los cuales serán desplegados en cada uno de los sitios de "LA CEAV".

3.3.3.1 UTM Tipo A Central

Equipo UTM (Unified Threat Management), Sistema de Seguridad Informática que sea del tipo Administración Unificada de Amenazas, donde se deberán ofrecer ya incluidas y listas para ser utilizadas, las funcionalidades que abajo se detallan, pudiendo ser todas ellas en una sola caja o en cajas diferentes.

Características del dispositivo

- El dispositivo debe ser un "appliance" de propósito específico "Hardware".



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Basado en tecnología ASIC "Application-Specific Integrated Circuit" y que sea capaz de brindar una solución de "Complete Content Protection". Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X o GNU/Linux.
- Capacidad de incrementar el rendimiento de VPN a través de soluciones en hardware dentro del mismo dispositivo (mediante el uso de un ASIC).
- Capacidad de reensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC).
- El equipo deberá poder ser configurado en modo Gateway o en modo transparente en la red.
- En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.

Características del Sistema operativo incluido

- Sistema operativo pre-endurecido específico para seguridad que sea compatible con el "appliance". Por seguridad y facilidad de administración y operación, no se aceptan soluciones sobre sistemas operativos genéricos.
- El sistema operativo debe incluir un servidor de DNS que permita resolver de forma local ciertas consultas de acuerdo con la configuración del administrador.

Firewall

- Las reglas de Firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
- Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall.
- Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino.
- Las reglas del firewall deberán tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando.
- Deberán poder definirse reglas de firewall para servicios sobre protocolo SCTP.



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Las acciones de las reglas deberán contener al menos el aceptar o rechazar la comunicación.
- Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.
- Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo que indique.
- Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año).
- Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.
- Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP).
- Capacidad de hacer traslación de direcciones estático, uno a uno, NAT.
- Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT.
- Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario).
- La solución deberá tener la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas.
- En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID.
- En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible.

Conectividad y Sistema de ruteo

- Funcionalidad integrada de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.
- Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs.
- Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.
- Soporte a políticas de ruteo (policy routing).
- El soporte a políticas de ruteo deberá permitir que, ante la presencia de dos enlaces a Internet, se pueda decidir cuál de tráfico sale por un enlace y qué tráfico sale por otro enlace.
- Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS.
- Soporte a ruteo dinámico RIPng, OSPFv3, BGP4+.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes.
- Soporte de ECMP (Equal Cost Multi-Path).
- Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas, pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador.
- Soporte de ECMP basado en comportamiento. En este modo, el tráfico será enviado de acuerdo a la definición de una ruta hasta que se alcance un umbral de tráfico. En este punto se comenzará a utilizar en paralelo una ruta alternativa.
- Soporte a ruteo de multicast.
- La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow.

VPN IPSec/L2TP/PPTP

- Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).
- Soporte para IKEv2 y IKE Configuration Method.
- Debe soportar la configuración de túneles L2TP.
- Debe soportar la configuración de túneles PPTP.
- Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES.
- Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits.
- Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.
- Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.
- Posibilidad de crear VPN's entre gateways y clientes con IPSec. esto es, VPNs IPSec site-to-site y VPNs IPSec client-to-site.
- La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN).
- En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall.
- Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.

VPN SSL

- Capacidad de realizar SSL VPNs.
- Soporte a certificados PKI X.509 para construcción de VPNs SSL.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.
- Soporte de renovación de contraseñas para LDAP y RADIUS.
- Soporte a asignación de aplicaciones permitidas por grupo de usuarios
- Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.
- Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL
- Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning).
- La VPN SSL integrada deberá soportar a través de algún plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS.
- Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL.
- Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente.
- Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios.
- Los portales personalizados deberán soportar al menos la definición de:
 - Widgets a mostrar.
 - Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC.
 - Esquema de colores.
 - Soporte para Escritorio Virtual.
 - Política de verificación de la estación de trabajo.
- La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información.
- En la configuración del Escritorio Virtual podrá definirse como mínimo:
 - La posibilidad de que el usuario cambie entre escritorio virtual y real.
 - La posibilidad de restringir el acceso a la memoria (clipboard) del escritorio virtual desde el escritorio real.
 - La posibilidad de utilizar medios removibles desde el escritorio virtual.
 - La posibilidad de acceder a recursos compartidos desde el escritorio virtual.
 - La posibilidad de imprimir desde el escritorio virtual.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA

- o La posibilidad de definir y restringir las aplicaciones que podrán ser ejecutadas en el escritorio virtual.

Traffic Shapping / QoS

- Capacidad de poder asignar parámetros de traffic shaping sobre reglas de firewall.
- Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión.
- Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general.
- Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo.
- Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo.
- Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia.

Autenticación y Certificación Digital

- Capacidad de integrarse con Servidores de Autenticación RADIUS.
- Capacidad nativa de integrarse con directorios LDAP.
- Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On".
- Capacidad de autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos TCP/UDP/ICMP. Debe de mostrar solicitud de autenticación (Prompt) al menos para Web (HTTP), FTP y Telnet.
- Mostrará solicitud de autenticación (Prompt) al menos para la Web (HTTP), FTP y Telnet.
- Debe ser posible definir puertos alternativos de autenticación para los protocolos http, FTP y Telnet.
- Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).
- Soporte a inclusión en autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol) y mediante archivos.
- Soporte de protocolo que permita revocar certificados OCSP (Online Certificate Status Protocol).
- La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Deben poder definirse usuarios y grupos en un repositorio local del dispositivo.
- Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo:
 - Longitud mínima permitida.
 - Restricciones de tipo de caracteres: numéricos, alfanuméricos, etc.
 - Expiración de contraseña.
- Capacidad de limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP.

Control de Endpoint

- La solución debe tener la capacidad de definir políticas que permitan analizar el estado de las estaciones de trabajo antes de permitir el acceso.
- Debe poder verificarse al menos los siguientes puntos:
 - Firewall personal instalado y activo.
 - Antivirus instalado y con versión de firmas actualizadas.
- La solución debe poder controlar las aplicaciones en la estación de trabajo. Como evaluación de la política deberá ser capaz de determinar si una aplicación debe estar instalada, no instalada, ejecutándose o no ejecutándose.
- Ante el incumplimiento de políticas la solución debe ofrecer la capacidad de bloquear el tráfico de dicho usuario o sólo alertarlo sobre el mismo.
- La solución debe brindar la posibilidad de redirigir el tráfico a un portal de remediación, cuando no se cumpla con alguna política de control de Endpoint.
- La evaluación de políticas podrá aplicarse mediante la instalación de un agente en la estación de trabajo.
- En caso de requerir un agente en la estación de trabajo, debe poder determinarse la mínima versión aceptada de dicho agente como parte de las políticas de Endpoint.
- Debe permitir la posibilidad de validar el estado de cumplimiento de políticas en el momento de establecer la sesión y forma periódica.

Alta Disponibilidad

- Posibilidad en Firewall Soporte a Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle.
- Alta Disponibilidad en modo Activo-Pasivo.
- Alta Disponibilidad en modo Activo-Activo.
- Posibilidad de definir al menos dos interfaces para sincronía.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red.
- Será posible definir interfaces de gestión independientes para cada miembro en un Cluster.

Características de Administración

- Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS).
- La interfaz gráfica de usuario (GUI) vía Web deberá estar en español y en inglés, configurable por el usuario.
- Interfaz basada en línea de comando (CLI) para administración de la solución.
- Puerto serial dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto.
- Comunicación cifrada y autenticada con username y password, tanto como para la interfaz gráfica de usuario como la consola de administración de línea de comandos (SSH o TELNET).
- El administrador del sistema podrá tener las opciones incluidas de autenticarse vía password y vía certificados digitales.
- Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden Administrar y realizar cambios de configuración.
- El equipo ofrecerá la flexibilidad para especificar que los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, TELNET, HTTP o HTTPS.
- El equipo deberá poder administrarse en su totalidad (Incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.
- Soporte de SNMP versión 2 y Soporte de SNMP versión 3.
- Soporte de al menos 3 servidores SYSLOG para poder enviar bitácoras a servidores de SYSLOG remotos.
- Soporte para almacenamiento de eventos en un repositorio que pueda consultarse utilizando SQL.
- Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.
- Monitoreo de comportamiento del "appliance" mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión.
- La interfaz gráfica de usuario (GUI) deberá de contar con la funcionalidad de autenticarse con un TOKEN (Autenticación de segundo factor) sin necesidad de integrar un equipo adicional o solución de otro fabricante.

Virtualización

- El dispositivo deberá poder virtualizar los servicios de seguridad mediante "Virtual Systems", "Virtual Firewalls" o "Virtual Domains".
- La instancia virtual debe soportar por lo menos funcionalidades de Firewall, VPN, URL Filtering, IPS y Antivirus.
- Se debe incluir la licencia para al menos 8 (ocho) instancias virtuales dentro de la solución a proveer.
- Cada instancia virtual debe poder tener un administrador independiente.
- La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales.
- Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red.
- Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual.
- Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual.
- Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual.

Capacidades de Desempeño:

- El equipo debe contar con un Throughput Firewall de al menos 7 Gbps.
- El equipo debe contar con un Throughput VPN IPSec de por lo menos 6 Gbps.
- El equipo debe contar con un Throughput IPS de al menos 2.5 Gbps.
- El equipo debe contar con un Throughput Antivirus en modo Proxy de al menos 1.2 Gbps y en modo Flow de al menos 2.4 Gbps.
- El equipo debe contar con al menos 5 millones de sesiones concurrentes.
- El equipo debe soportar al menos 190,000 nuevas sesiones por segundo.
- El equipo deberá de contar desde un inicio con la funcionalidad y licenciamiento de por lo menos 450 usuarios de SSL VPN.

Características de Hardware:

- El equipo debe contar con al menos 5 Interfaces GigaEthernet RJ45.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA

- El equipo debe contar con al menos 1 Interfaces Rj45 para Consola de Admon.
- El equipo debe contar con al menos 3 Interfaces 1000Base-X (SFP).
- El equipo debe contar con al menos 100 GB de Almacenamiento Interno.
- El equipo debe contar con al menos con un puerto USB.

3.3.3.2 UTM Tipo B Remoto

Equipo UTM (Unified Trade Managment), Sistema de Seguridad informática que sea del tipo Administración Unificada de Amenazas, donde se deberán ofrecer ya incluidas y listas para ser utilizadas, las funcionalidades que abajo se detallan, pudiendo ser todas ellas en una sola caja o en cajas diferentes.

Características del dispositivo

- El dispositivo debe ser un "appliance" de propósito específico "Hardware".
- Basado en tecnología ASIC "Application-Specific Integrated Circuit" y que sea capaz de brindar una solución de "Complete Content Protection". Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X o GNU/Linux.
- Capacidad de incrementar el rendimiento de VPN a través de soluciones en hardware dentro del mismo dispositivo (mediante el uso de un ASIC).
- Capacidad de reensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC).
- El equipo deberá poder ser configurado en modo Gateway o en modo transparente en la red.
- En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.

Características del Sistema operativo incluido

- Sistema operativo pre-endurecido específico para seguridad que sea compatible con el "appliance". Por seguridad y facilidad de administración y operación, no se aceptan soluciones sobre sistemas operativos genéricos.
- El sistema operativo debe incluir un servidor de DNS que permita resolver de forma local ciertas consultas de acuerdo a la configuración del administrador.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

Firewall

- Las reglas de Firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
- Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall.
- Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino.
- Las reglas del firewall deberán tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando.
- Deberán poder definirse reglas de firewall para servicios sobre protocolo SCTP.
- Las acciones de las reglas deberán contener al menos el aceptar o rechazar la comunicación.
- Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.
- Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo que indique.
- Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año).
- Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.
- Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP).
- Capacidad de hacer traslación de direcciones estático, uno a uno, NAT.
- Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT.
- Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario).
- La solución deberá tener la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas.
- En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID.



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible.

Conectividad y Sistema de ruteo

- Funcionalidad integrada de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.
- Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs.
- Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.
- Soporte a políticas de ruteo (policy routing).
- El soporte a políticas de ruteo deberá permitir que, ante la presencia de dos enlaces a Internet, se pueda decidir cuál de tráfico sale por un enlace y qué tráfico sale por otro enlace.
- Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS.
- Soporte a ruteo dinámico RIPng, OSPFv3, BGP4+.
- La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes.
- Soporte de ECMP (Equal Cost Multi-Path).
- Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas, pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador.
- Soporte de ECMP basado en comportamiento. En este modo, el tráfico será enviado de acuerdo a la definición de una ruta hasta que se alcance un umbral de tráfico. En este punto se comenzará a utilizar en paralelo una ruta alternativa.
- Soporte a ruteo de multicast.
- La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow.

VPN IPSec/L2TP/PPTP

- Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).
- Soporte para IKEv2 y IKE Configuration Method.
- Debe soportar la configuración de túneles L2TP.
- Debe soportar la configuración de túneles PPTP.
- Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES.
- Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits.
- Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.
- Posibilidad de crear VPN's entre gateways y clientes con IPSec. esto es, VPNs IPSec site-to-site y VPNs IPSec client-to-site.
- La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN).
- En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall.
- Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.

VPN SSL

- Capacidad de realizar SSL VPNs.
- Soporte a certificados PKI X.509 para construcción de VPNs SSL.
- Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.
- Soporte de renovación de contraseñas para LDAP y RADIUS.
- Soporte a asignación de aplicaciones permitidas por grupo de usuarios.
- Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.
- Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL.
- Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning).
- La VPN SSL integrada deberá soportar a través de algún plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS.
- Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL.
- Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente.
- Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios.
- Los portales personalizados deberán soportar al menos la definición de:
 - Widgets a mostrar.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA

- o Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC.
- o Esquema de colores.
- o Soporte para Escritorio Virtual.
- o Política de verificación de la estación de trabajo.

La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información. En la configuración del Escritorio Virtual podrá definirse como mínimo:

- La posibilidad de que el usuario cambie entre escritorio virtual y real.
- La posibilidad de restringir el acceso a la memoria (clipboard) del escritorio virtual desde el escritorio real.
- La posibilidad de utilizar medios removibles desde el escritorio virtual.
- La posibilidad de acceder a recursos compartidos desde el escritorio virtual.
- La posibilidad de imprimir desde el escritorio virtual.
- La posibilidad de definir y restringir las aplicaciones que podrán ser ejecutadas en el escritorio virtual.

Traffic Shapping / QoS

- Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall.
- Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión.
- Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general.
- Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo.
- Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo.
- Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia.

Autenticación y Certificación Digital

- Capacidad de integrarse con Servidores de Autenticación RADIUS.
- Capacidad nativa de integrarse con directorios LDAP.
- Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA

preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On".

- Capacidad de autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos TCP/UDP/ICMP. Debe de mostrar solicitud de autenticación (Prompt) al menos para Web (HTTP), FTP y Telnet.
- Debe ser posible definir puertos alternativos de autenticación para los protocolos http, FTP y Telnet.
- Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).
- Soporte a inclusión en autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol) y mediante archivos.
- Soporte de verificación de validación de certificados digitales mediante el protocolo OSCP (Online Simple Enrollment Protocol).
- La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.
- Deben poder definirse usuarios y grupos en un repositorio local del dispositivo.
- Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo:
 - Longitud mínima permitida.
 - Restricciones de tipo de caracteres: numéricos, alfanuméricos, etc.
 - Expiración de contraseña.
- Capacidad de limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP.

Control de Endpoint

- La solución debe tener la capacidad de definir políticas que permitan analizar el estado de las estaciones de trabajo antes de permitir el acceso.
- Debe poder verificarse al menos los siguientes puntos:
 - Firewall personal instalado y activo.
 - Antivirus instalado y con versión de firmas actualizadas.
- La solución debe poder controlar las aplicaciones en la estación de trabajo. Como evaluación de la política deberá ser capaz de determinar si una aplicación debe estar instalada, no instalada, ejecutándose o no ejecutándose.
- Ante el incumplimiento de políticas la solución debe ofrecer la capacidad de bloquear el tráfico de dicho usuario o sólo alertarlo sobre el mismo.
- La solución debe brindar la posibilidad de redireccionar el tráfico a un portal de remediación, cuando no se cumpla con alguna política de control de Endpoint.



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- La evaluación de políticas podrá aplicarse mediante la instalación de un agente en la estación de trabajo.
- En caso de requerir un agente en la estación de trabajo, debe poder determinarse la mínima versión aceptada de dicho agente como parte de las políticas de Endpoint.
- Debe permitir la posibilidad de validar el estado de cumplimiento de políticas en el momento de establecer la sesión y forma periódica.

Alta Disponibilidad

- Posibilidad en Firewall Soporte a Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle.
- Alta Disponibilidad en modo Activo-Pasivo.
- Alta Disponibilidad en modo Activo-Activo.
- Posibilidad de definir al menos dos interfaces para sincronía.
- El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red.
- Será posible definir interfaces de gestión independientes para cada miembro en un Cluster.

Características de Administración

- Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS).
- La interfaz gráfica de usuario (GUI) vía Web deberá estar en español y en inglés, configurable por el usuario.
- Interfaz basada en línea de comando (CLI) para administración de la solución.
- Puerto serial dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto.
- Comunicación cifrada y autenticada con username y password, tanto como para la interfaz gráfica de usuario como la consola de administración de línea de comandos (SSH o TELNET).
- El administrador del sistema podrá tener las opciones incluidas de autenticarse vía password y vía certificados digitales.
- Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden Administrar y realizar cambios de configuración.
- El equipo ofrecerá la flexibilidad para especificar que los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, TELNET, HTTP o HTTPS.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.
- Soporte de SNMP versión 2 y Soporte de SNMP versión 3.
- Soporte de al menos 3 servidores SYSLOG para poder enviar bitácoras a servidores de SYSLOG remotos.
- Soporte para almacenamiento de eventos en un repositorio que pueda consultarse utilizando SQL.
- Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.
- Monitoreo de comportamiento del "appliance" mediante SNMP; el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.
- Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión.
- La interfaz gráfica de usuario (GUI) deberá de contar con la funcionalidad de autenticarse con un TOKEN (Autenticación de segundo factor) sin necesidad de integrar un equipo adicional o solución de otro fabricante.

Virtualización

- El dispositivo deberá poder virtualizar los servicios de seguridad mediante "Virtual Systems", "Virtual Firewalls" o "Virtual Domains".
- La instancia virtual debe soportar por lo menos funcionalidades de Firewall, VPN, URL Filtering, IPS y Antivirus.
- Se debe incluir la licencia para al menos 8 (ocho) instancias virtuales dentro de la solución a proveer.
- Cada instancia virtual debe poder tener un administrador independiente.
- La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales.
- Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red.
- Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual.
- Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual.
- Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual.

Capacidades de Desempeño:



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- El equipo debe contar con un Throughput Firewall de al menos 1.4 Gbps.
- El equipo debe contar con un Throughput VPN IPsec de por lo menos 900 Mbps.
- El equipo debe contar con un Throughput IPS de al menos 200 Mbps.
- El equipo debe contar con un Throughput AntiVirus en modo Proxy de al menos 30 Mbps y/o en modo Flow de al menos 45 Mbps.
- El equipo debe contar con al menos 450,000 de sesiones concurrentes.
- El equipo debe soportar al menos 3500 Nuevas sesiones por segundo.
- El equipo deberá de contar desde un inicio con la funcionalidad y licenciamiento de por lo menos 100 Usuarios de VPN por SSL.

Características de Hardware:

- El equipo debe contar con al menos 6 Interfaces GigaEthernet RJ45.
- El equipo debe contar con al menos 2 Interfaces GigaEthernet de WAN.
- El equipo debe contar con al menos 15 GB de Almacenamiento Interno.
- El equipo debe contar con al menos con un puerto USB.

3.3.3.3 Cliente UTM para PC para preservar políticas corporativas

"EL PROVEEDOR" adjudicado deberá proporcionar mínimo 15 clientes de software que puedan ser instalados en dispositivos Windows, MAC OS X, IOS y Android, deberán interactuar con los equipos UTM solicitados. Las características mínimas a cumplir se describen a continuación.

Solución endpoint security que incluye todo en uno que ayuda a proteger los dispositivos del usuario final permitiendo extender la seguridad del UTM al dispositivo del usuario final.

Características del endpoint

La solución de endpoint deberá contar por lo menos con:

- Anti-malware (antivirus).
- Application Firewall.
- Web Filter.
- Vulnerability management.
- Two-factor authentication.
- Remote access (VPN) que soporte protocolo IPsec y SSL.

Deberá soportar por lo menos los siguientes sistemas operativos:



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Windows,
- Mac OS X,
- iOS,
- Android,

Las políticas del endpoint deberán poder ser administradas desde la consola del UTM y no se requiere tener un servidor dedicado para esto,

Deberá soportar la administración de por lo menos 600 clientes end points.

Los modos de instalación del endpoint en los equipos deber soportar por lo menos:

- Manual interactivo,
- Manual silencioso,
- Por medio de GPO de Active Directory,
- Mediante una herramienta de distribución (de terceros).

En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.

Control de Endpoint

La solución debe tener la capacidad de definir políticas que permitan analizar el estado de las estaciones de trabajo antes de permitir el acceso.

Debe poder verificarse al menos los siguientes puntos:

- Firewall personal instalado y activo.
- Antivirus instalado y con versión de firmas actualizadas.
- La solución debe poder controlar las aplicaciones en la estación de trabajo. Como evaluación de la política deberá ser capaz de determinar si una aplicación debe estar instalada, no instalada, ejecutándose o no ejecutándose,
- Ante el incumplimiento de políticas la solución debe ofrecer la capacidad de bloquear el tráfico de dicho usuario o sólo alertarlo sobre el mismo.
- La solución debe brindar la posibilidad de redireccionar el tráfico a un portal de remediación, cuando no se cumpla con alguna política de control de Endpoint.
- La evaluación de políticas podrá aplicarse mediante la instalación de un agente en la estación de trabajo.
- En caso de requerir un agente en la estación de trabajo, debe poder determinarse la mínima versión aceptada de dicho agente como parte de las políticas de Endpoint.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Debe permitir la posibilidad de validar el estado de cumplimiento de políticas en el momento de establecer la sesión y forma periódica.

3.3.4 Servicios de telefonía IP

"EL PROVEEDOR" deberá de instalar al menos 500 Servicios de telefonía IP en los diferentes inmuebles de "LA CEAV", que serán repartidos en los diferentes inmuebles mediante un plan que "LA CEAV" le entregará a "EL PROVEEDOR". Así mismo deberá proporcionar servicios de Mensajería unificada, Colaboración y Centro de Contacto que permitan efficientar las actividades de los funcionarios de "LA CEAV".

3.3.4.1 Características del sistema de telefonía IP

Especificaciones Técnicas Mínimas que debe cubrir el Administrador de llamadas de telefonía IP

La solución deberá ofrecer como mínimo el soporte de los siguientes servicios:

- Procesamiento centralizado.
- Alta Disponibilidad en una configuración activo-pasivo que permita que al existir un corte de algunos de los servidores las comunicaciones de voz establecidas no se corten.
- Administración centralizada.
- Gateways distribuidos.
- Módulos de Supervivencia.
- Soporte de teléfonos IP.
- Soporte de teléfonos IP en software.
- Soporte de líneas analógicas.
- Soporte de extensiones H.323, SIP, digitales y analógicas de manera simultánea en el mismo servidor.
- Soporte de 802.3af en todos los teléfonos IP.
- Soporte de encriptación en teléfonos IP por medio de AES-128/TLS.
- Soporte de troncales analógicas, E&M, E1, H.323 y SIP.
- Servicios de mensajería unificada (integración de correo de voz, correo electrónico y mensajes de fax en un mismo buzón).
- Servicios de colaboración para usuarios ejecutivos que puedan ser accedidos desde distintos dispositivos de usuario (teléfono de escritorio, PC personal, tableta electrónica, o smartphone), con la posibilidad de mezclar diversos tipos de medios de comunicación como voz, Mensajería instantánea, intercambio de archivos y aplicaciones y que permita la fácil adición de participantes incluso por distintos medios de comunicación.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Sistema de gestión y administración que permita la fácil gestión y configuración de servicios incluyendo aquellos que tengan que ver con las comunicaciones unificadas solicitadas.
- Sistema de Monitoreo y reporteo del sistema que brinde visibilidad del rendimiento del sistema, tráfico de llamadas, alarmas del sistema, visibilidad del consumo telefónico que sea capaz de generar diversos reportes de estos indicadores.
- Sistema de tarificación que permita llevar un control del gasto telefónico sobre los enlaces a la red pública.

Todos los componentes antes mencionados, a excepción del tarifador, preferentemente deberán ser de la misma marca del servidor de Telefonía para una plena integración y operación.

El Administrador de llamadas de telefonía IP deberá cumplir como mínimo con las siguientes características:

- La arquitectura deberá estar basada en un arreglo de un Administrador de telefonía IP con procesamiento de las llamadas y administración centralizada y con capacidad de distribuir en los sitios remotos dispositivos gateways, utilizando el protocolo IP.
- El Administrador de llamadas de telefonía IP estará formado por un controlador de llamadas central y al cual se le podrán asociar gabinetes con funciones de Gateway con espacio para alojar extensiones analógicas e IP, o consistir de un solo sistema que realiza ambas funciones.
- La comunicación entre el controlador de llamadas central y los gateways del sitio central se realizará a través de la red de datos LAN y de igual modo, los gateways para cumplir la capacidad solicitada se conectarán por TCP/IP mediante puertos 10/100/1000 BaseTX, en el caso de requerir conectar localidades remotas, los gateways se conectarán por IP haciendo tráfico sobre la red WAN.
- El Administrador de llamadas de telefonía IP deberá soportar capacidad de crecimiento en un sólo Administrador de llamadas de hasta 12,000 usuarios o hasta 50,000 en un ambiente de clúster.
- El Administrador de Llamadas de Telefonía IP deberá proveer una disponibilidad de al menos 99.5% comprobable.
- El Administrador de llamadas de telefonía IP deberá soportar como mínimo capacidad de hasta 300 mil llamadas completadas en hora pico (BHCC), en una solución 100% IP. Este número tendrá que ser comprobado en base a la documentación oficial del fabricante.
- El Administrador de llamadas deberá soportar su instalación en un entorno de servidores virtuales basados en VMWare o similar para su incorporación en un ambiente de data center en caso de ser necesario.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- El Administrador de llamadas de Telefonía IP deberá de operar en modo Hot-Standby con un administrador redundante con la misma configuración y nivel de servicios del servidor principal.
- El Administrador de llamadas de Telefonía IP debe soportar conexión de gateways remotos mediante la WAN, se requiere que soporte como mínimo un total de 200 gateways remotos asignados a un solo administrador de llamadas de telefonía IP.
- La Administración de las extensiones en los gateways remotos deberá realizarse únicamente en el sitio central.
- El Administrador de llamadas de telefonía IP deberá contar con la capacidad de sincronizar la información de configuración con los gateways remotos en el momento que el administrador del sistema lo requiera. No se deberá requerir configurar las extensiones en ambos sitios.
- El Sistema Operativo del Administrador de llamadas de Telefonía IP deberá estar basado en una arquitectura abierta y estándar, de preferencia basada en sistema Operativo Linux o Unix, además soportar su instalación en un entorno de virtualización.
- Para el proyecto deberá considerarse la última versión de software de procesamiento de llamadas disponible en el mercado, dicho software debe incluir soporte de los protocolos de red ISDN, QSIG, Tie Line E&M, IP, H323, SIP. También deberá considerarse todas las actualizaciones de software, incluyendo el hardware, que se liberen durante la vigencia del contrato sin costo adicional para "LA CEAV".
- El controlador de llamadas del administrador de llamadas de Telefonía IP deberá soportar conexión a la red LAN mediante conexión 10/100/1000BaseTx.
- El controlador de llamadas del sistema de telefonía IP deberá estar basado en hardware estándar del mercado (servidores estándar), es decir no se aceptarán soluciones basadas en appliances propietarios.
- El Administrador de Llamadas de Telefonía IP deberá ser capaz de administrarse de manera local y remota. La administración del sistema deberá ser vía TCP/IP y vía módem. En ambos casos debe proveerse un medio de conexión seguro para la administración.
- El Administrador de Llamadas de Telefonía IP deberá administrarse desde el sistema de gestión y administración centralizada provista por la solución propuesta, este sistema debe proveer una interfaz gráfica para la gestión del sistema que permita el acceso seguro de los administradores.
- El Administrador de llamadas de telefonía IP deberá soportar diferentes tipos de tróncales hacia la red pública. - tróncales Digitales El G.703 R2 MFC, tróncales Digitales ISDN (PRI y BRI), tróncales analógicas (C.O.) y SIP.
- El sistema deberá generar registros CDR para el control de la tarificación de llamadas.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA

- Los registros de CDR para tarificación deberán ser enviados a través del protocolo IP, garantizando mediante el uso de protocolos a nivel de la capa de la aplicación que los registros de los datos son enviados y recibidos correctamente.

La redundancia requerida en el Sitio Principal deber ser la siguiente:

- Deberá incluir como mínimo redundancia en el procesador principal, de manera que ante la pérdida del procesador activo entrará automáticamente el procesador de respaldo. El procesador de respaldo deberá sincronizarse con el procesador principal en tiempo real, de manera que, en caso de falla del procesador principal, el tiempo de recuperación del procesador de respaldo sea inmediato, sin tiempo de retardo, capaz de recuperar todos los servicios de telefonía en caso de que suceda lo anterior mencionado. De esta forma todas las llamadas activas al momento de la falla no deben perderse.
- La Redundancia entre los Servidores de Telefonía IP debe soportar todos los servicios disponibles del servidor principal.
- Se deberá tener actualización en tiempo real de los cambios en la configuración entre el servidor principal y el secundario.
- La redundancia provista deberá manejar mecanismos que permitan mantener homogénea la base de datos entre los servidores del sistema. Deberá proveer al menos un mecanismo automático y otro manual.

En el momento de falla del servidor principal, todas las llamadas deben permanecer en curso sin ninguna interrupción, además todos los gateways y terminales tendrán que ser controlados por el servidor redundante.

Facilidades básicas que deberá proporcionar el Administrador de Llamadas de telefonía IP:

- Transferencia de llamadas.
- Anuncio de altavoz en los teléfonos que lo soporten.
- Rellamada sobre extensión ocupada.
- Configuración de clases de servicio en extensiones y troncales para acceso a PSTN.
- Restricción de llamadas de salida.
- Transferencia de una llamada externa.
- Remarcación del último número marcado.
- Conferencias tripartitas.
- Conferencias de voz para más de 6 participantes con acceso vía un código de conferencia.



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Capacidad instalada de generar al menos 3 conferencias telefónicas de 20 participantes con acceso vía un código de conferencia.
- Transferencia interna y externa.
- Llamada en espera.
- Rellamada.
- Solicitud de Rellamada.
- Marcación vía directorio en los teléfonos IP.
- Búsqueda en directorios externos con formato LDAP.
- Retención de llamada/llamada en espera.
- Intercomunicador.
- Funcionalidad jefe-Secretaría.
- Operadora Automática.
- Consola de Operadora.
- Anuncios vocales.
- Recordatorio de cita.
- Encriptación de llamadas.
- Grupos de captura de llamadas.
- Debe permitir la intercalación en una comunicación establecida (contestar una llamada en el transcurso de otra).
- Desvío de llamadas activado por el usuario.
- Desvío de llamadas en ocupado.
- Desvío en no contesta.
- Configuración de códigos de autorización, de hasta 6 dígitos, para realizar llamadas de larga distancia, llamadas a celulares. (Código se case con el usuario).
- Servicio Nocturno.
- Se requiere que el Administrador de llamadas de telefonía IP soporte como mínimo aplicaciones de correo de voz, mensajería unificada, centro de atención de llamadas (call center) basado en IP con terminales de agentes basados en teléfono de escritorio o softphone.
- Deberá soportar un plan de numeración interno totalmente programable y flexible, mínimo de 8 dígitos.
- Deberá contar la posibilidad de selección automática de ruta o Ruta de Menor Costo.
- Deberá soportar capacidad para manejar troncales H.323 y troncales SIP.
- Deberá soportar los servicios de Proxy SIP y Gatekeeper H.323.
- Deberá incluir un servicio de colaboración audio bridge.
- El sistema deberá soportar la capacidad de dar a los empleados un número de reservación para conferencia personal con acceso controlado y seguro, el cual podrá ser previamente programado.
- Deberá soportar servicios de directorio con posibilidad de integración con directorios externos tipo LDAP como Active Directory de MS.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Soportar mecanismo de CAC hacia los sitios remotos para uso optimizado del ancho de banda
- Las troncales IP deberán contar con la capacidad de ser comprimidas con los algoritmos de compresión G.729, G.723, G.722 y G.711.
- Deberá soportar la conexión con troncales SIP de forma segura por medio de TLS.
- Deberá proveer servicios de trazado de los distintos protocolos soportados para el análisis y solución de problemas.
- Deberá proveer servicios de seguridad que impidan conexiones y sesiones de comunicación con dispositivos no autorizados.
- Deberá incluir el servicio de DHCP para asignación dinámica de direccionamiento IP para los teléfonos de la solución.
- Deberá incluir el servicio de música en espera que se deberá escuchar por el llamante cuando éste sea puesto en retención. Debe proveerse la posibilidad de que la fuente de esta música este dentro del sistema o pueda ser una fuente externa como un reproductor.
- El Administrador de Llamadas de Telefonía IP deberá permitir que en cualquiera de sus gabinetes o gateways locales, se puedan utilizar de manera local los anuncios y fuentes de música en espera. De manera que exista un mecanismo que permita escoger la fuente de audio que esté más cercana al punto de ingreso en donde el llamante requirió el audio.
- Debe estar basado en estándares, la solución debe quedar operando bajo protocolos estándares, por lo cual se debe garantizar que los teléfonos IP, Administrador de llamadas de telefonía IP y gateways como mínimo pueden trabajar con cualquier marca de switches LAN y routers para la WAN basados en estándares.
- Los Protocolos y estándares que deberá proporcionar el Administrador de Llamadas de telefonía IP deben ser al menos:
 - TCP/IP, UDP, DHCP y SNMP V3.
 - SIP v2.
 - LDAP.
 - 802.1p, 802.1Q, DiffServ, RTP, RTCP,
 - AES ó 3DES ó DES.
 - H.323 v2 o superior, H.225, H.245.
 - Fax Grupo 3, T.38.
 - Codecs de compresión en G.722, G723, G.729a/b, G711.
 - HTTPS y SSH.
 - LLDP.

El Administrador de Llamadas de telefonía IP debe soportar la capacidad de integrar las siguientes aplicaciones:



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- El Software de Centro de Llamadas (Call Center) ACD el cual deberá residir en el Administrador de Llamadas de telefonía IP o con un módulo externo. Deberá ofrecer capacidad de crecimiento en un solo Administrador de llamadas de hasta 500 agentes.
- Debe permitir el equipamiento de agentes por medio de teléfonos IP o por medio de Softphones.
- Para la aplicación de Centro de llamadas debe proveer al menos servicios de tipo inbound en la configuración mínima siendo posible adicionar módulos que permitan agregar servicios de Outbound, integración con CRM e integración con IVR en un futuro.
- El equipo ofertado deberá contar de inicio sólo con interacciones de voz y debe permitir que, en un futuro, puedan integrarse interacciones de chat, email y redes sociales.
- Debe proveer estadísticas de la aplicación de Centro de llamadas y una interfaz de administrador.
- CTI (Computing & Telephony Integration) mediante el soporte de los estándares CSTA, TAPI, TSAPI o JTAPI para integración con aplicaciones de terceros.
- Servicios de Telefonía que permita el control de la llamada sobre servicios estándares Web SOAP/XML.
- Deberá soportar SIP con funciones de registro/Proxy, presencia y Redirect. El Administrador de Llamadas de telefonía IP, deberá también soportar el registro de terminales SIP de diferentes fabricantes.
- Grabador de llamadas, que soporte grabación simultánea de todos los agentes. Posibilidad de expansión y grabación de pantallas.

Características técnicas mínimas que deberá de cumplir el Gateway:

- Deberá ser de la misma marca de la solución global de telefonía y operar bajo el mismo sistema operativo. Con esto se garantizará la plena compatibilidad de todos los componentes, así como su correcta operación.
- Deberá ser un Gateway dedicado a funciones de telefonía.
- Deberá proveer al menos un puerto 10/100/1000 BT para su conexión a la red LAN del sitio.
- El Gateway debe soportar terminales analógicas, digitales e IP, así como el soporte de troncales analógicas y digitales ISDN BRI, ISDN PRI, E1 R2, H323 y E&M analógico.
- Deberá estar equipado con un respaldo de energía de al menos 4 horas en caso de fallas de C.A. a través de un sistema de UPS o con un banco de baterías dedicado a esta función.



CEAV
COMISION EJECUTIVA
DE ATENCION A VICTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

Deberá contar con capacidad instalada de 2 E1's R2 MFC equipados en tarjetas independientes y con capacidad de crecimiento de hasta 8 E1's.

Deberá contar con capacidad de montaje a piso o en rack.

Deberá contar con capacidad de alojar mínimo 500 extensiones de cualquier tipo.

- El Sistema Operativo del dispositivo con funciones de gateway deberá ser de arquitectura abierta y estándar, no se aceptan soluciones basadas en sistema operativo windows.
- Deberá incluir todos los circuitos de compresión VoIP necesarios para la correcta operación.
- Debe Incluir servicio de operadora automática de manera local en cada uno de los gateways.
- Debe Incluir servicio de anuncios por localidad.
- Debe incluir servicio de música en espera de forma local.
- El Gateway remoto debe incluir el software necesario para soportar Selección de Ruta Alterna.

3.3.4.2 Mensajería Unificada

Se requiere una solución de mensajería unificada para todos los usuarios con una aplicación centralizada que proporcione servicio a usuarios a nivel metropolitano y nacional, operándose y administrándose desde los sitios principales, que permita integración de los servicios de correo de voz.

Se Busca una Arquitectura Robusta que contemple la ciudad de México e interior de la República, que sea Modular y Flexible, basada en estándares que permitan el Crecimiento para nuevos usuarios, así como para nuevas aplicaciones, tales como correo electrónico y Servidor de Fax, **"EL PROVEEDOR"** debe soportar la Mensajería Unificada, siendo 100% compatible con la Infraestructura de Conmutadores propuesta por **"EL PROVEEDOR"**.

"EL PROVEEDOR" deberá proponer un esquema de mensajería unificada, indicando claramente la arquitectura y sistema operativo propuesto, en el entendido que será su responsabilidad la administración del servicio y que al menos proporcione a los empleados funciones de buzón de voz avanzadas, integración del correo electrónico, conforme a lo siguiente:

1. **"LA CEAV"**, requiere una solución de mensajería unificada de última generación, que permita al usuario acceder a sus mensajes en cualquier momento y lugar, para lo cual todos los mensajes de voz, o correo electrónico tendrán disponibilidad a través de sus dispositivos móviles, en



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

el escritorio de una computadora o vía Web de manera remota, implementando esquemas de seguridad, deberá ser compatible principalmente con Exchange de Microsoft.

2. Deberá contar con una gestión visual de los mensajes, es decir, que el usuario pueda ver sus mensajes y decidir cuál desea revisar.
3. La propuesta de solución deberá permitir al usuario el control de su buzón ya sea a través de su aparato telefónico, por medio de una interfaz web en una PC o por medio de los clientes de comunicación en dispositivos móviles y "LA CEAV" podrá definir capacidades de buzón para perfiles de usuario.
4. El sistema de correo de voz deberá permitir a los usuarios realizar grabaciones bajo demanda de sus llamadas de voz y que estos se almacenen en formato WAV para su posterior consulta.

3.3.4.3 Servicio de audio conferencia

"EL PROVEEDOR" prestará un servicio de audio conferencias que provea al menos las siguientes funcionalidades:

- Deberá tener un sistema de programación de audio conferencia con la posibilidad de establecer conferencias programadas y sobre demanda.
- El sistema de conferencias programadas y sobre demanda debe de integrarse con el sistema de telefonía por conexión SIP. No se acepta interconexiones TDM.
- El sistema de audio conferencias programadas y sobre demanda debe permitir conferencias de audio entre los usuarios internos y usuarios externos que están en la red pública.
- El sistema de conferencias programadas deberá soportar al menos 30 puertos de audio, donde no hay límites de grupos de conferencia simultáneas dentro del grupo de los puertos disponibles, esto quiere decir que se puede generar una conferencia de hasta 30 personas, 3 conferencias simultáneas con hasta 10 personas, 6 conferencias simultáneas con hasta 5 personas, etc.
- El sistema de conferencia debe proveer la posibilidad de hacer conferencias agendadas o conferencia sobre demanda.
- El sistema de conferencia debe permitir que los usuarios puedan indicar su nombre antes de acceder al bridge de audio conferencia.
- El sistema de conferencia programada debe proveer una interfaz web para programación de las conferencias.



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- La interfaz de programación de conferencias debe ser soportada en web browsers como Internet Explorer, Firefox y Safari.
- La interfaz de programación y acceso a la conferencia debe poder proveerse sobre tabletas electrónicas.
- La programación de la conferencia debe tener la posibilidad de seleccionar fecha, horario, zona horaria, nombre de la conferencia y código de la conferencia.
- Deberá tener mensajes pre-programados de email e invitaciones de calendario con la información del número del bridge de audio y código de acceso.
- Deberá tener la posibilidad de invitar a los participantes como líderes ó invitados con diferentes perfiles de acceso y control de la sesión.
- Los líderes deberán tener control de todos los servicios de la conferencia como: agregar participante, quitar participante, poner en mudo a un participante específico, poner en mudo a todos los participantes, poner un participante específico "on hold", poner a todos los participantes "on hold".
- Los participantes en la condición de invitado tienen solamente la opción de acceder a la conferencia y escuchar y hablar conforme lo modere el líder
- El sistema de conferencias programadas deberá proveer una aplicación de chat/mensajería instantánea vía web entre los usuarios del servicio de conferencia con cuenta asignada en el sistema.
- La aplicación de chat/mensajería instantánea debe estar integrada en la misma pantalla del control de los servicios de conferencia de audio.
- La aplicación de Chat permitirá que los usuarios del sistema puedan intercambiar mensaje durante una conferencia en curso.

3.3.4.4 Especificaciones Técnicas Mínimas que deben cubrir los Gateway para sitio remoto

Con el fin de que la solución propuesta se base en plataforma distribuida con procesamiento centralizado se contempla la puesta en operación de equipamiento con funciones de Gateway para las localidades remotas, las cuales en un inicio deben permitir una migración transparente de la red y los sistemas de telefonía actuales a un esquema de telefonía IP convergente, para lo cual a continuación se describen las necesidades de los gateways remotos.

Deberá de cumplir mínimo con las siguientes características:

- Deberá ser de la misma marca de la solución global de telefonía y operar bajo el mismo sistema operativo. Con esto se garantizará la plena compatibilidad de todos los componentes, así como su correcta operación.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA

- Deberá ser un Gateway dedicado a funciones de telefonía.
- Deberá proveer al menos un puerto 10/100/1000 BT para su conexión a la red LAN del sitio.
- El Gateway debe soportar terminales analógicas e IP, así como el soporte de troncales analógicas y digitales ISDN BRI, ISDN PRI, E1 R2 y H323.
- Deberá soportar alimentación de poder en DC y/o AC.
- Deberá estar equipado con un respaldo de energía de al menos 4 horas en caso de fallas de C.A. a través de un sistema de UPS o con un banco de baterías dedicado a esta función.
- El Sistema Operativo del dispositivo con funciones de gateway deberá ser de arquitectura abierta y estándar.
- La solución de telefonía IP propuesta para los gateways debe contar con soporte de encriptación de llamadas entre los diferentes gateways a través de 3DES o AES.
- Debe tener conectividad a la PSTN (Red conmutada) con tarjetas tipo E1 o de puertos de Troncal Analógica.
- Deberá soportar señalización R2 MFC e ISDN PRI y BRI.
- Deberá incluir todos los circuitos de compresión VoIP necesarios para la correcta operación.
- El Gateway remoto deberá tener un módulo de supervivencia local para que, en caso de falla de la conectividad al sitio central, el Gateway pueda funcionar como dispositivo independiente y administrar sus propios recursos de Telefonía en caso de falla del enlace o conectividad al Administrador de Llamadas de telefonía IP central, conservando los servicios telefónicos que se brindan en modo de operación normal.
- En modo de supervivencia deberá ser posible establecer llamadas a otros sitios por medio de la PSTN marcando de forma normal por extensión, este servicio deberá ser transparente para los usuarios.
- La solución de supervivencia para los sitios remotos debe proveer la generación de CDR para que en caso de pérdida de comunicación entre el Gateway remoto y el sitio central esta información no se pierda y pueda consolidarse una vez restablecida la comunicación.
- Los cambios y modificaciones en el Gateway se deberán realizar en el sitio Central y las actualizaciones hacia el gateway podrán ser realizadas en forma calendarizada y automática cuando se sincronicen los sistemas nuevamente.
- La administración del Gateway deberá ser realizada a través del Software de Administración del Administrador de Llamadas de Telefonía IP Central (Sistema de gestión y Administración centralizado).
- Deberá soportar los mismos aparatos telefónicos analógicos e IP que utiliza el Administrador de Llamadas de Telefonía IP Central y brindar el mismo nivel de servicios del sitio central.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Una extensión ubicada en el sitio remoto (gateway remoto) no debe ser necesario darse de alta en ambos sitios, con darse de alta en una sola localidad debe ser suficiente.
- La conexión al Administrador de Llamadas de Telefonía IP, debe realizarse mediante un puerto Ethernet; mediante el protocolo TCP/IP, el procesamiento deberá ser centralizado, es decir el Gateway remoto deberá conservarse como extensión del Administrador de Llamadas de Telefonía IP Central, excepto en los casos de pérdida del enlace en donde el gateway deberá tener capacidad de operación autónoma brindando el mismo nivel de servicios que en modo de operación normal.
- Debe incluir servicio de operadora automática de manera local en cada uno de los gateways.
- Debe incluir servicio de anuncios por localidad.
- Debe incluir servicio de música en espera de forma local.
- El Gateway debe ser montable en rack.
- El Gateway remoto debe incluir el software necesario para soportar Selección de Ruta Alterna.

3.3.4.5 Aparatos Telefónicos IP Básico

Los teléfonos IP Básico con switch integrado deben incorporar las siguientes funciones mínimas:

- Incluir pantalla de al menos cuatro líneas de apariencia, monocromática, retroiluminada.
- Altavoz de manos libres full-duplex con cancelación de eco.
- Mínimo 10 teclas de función.
- Hasta 30 teclas programables cuya información deberá estar almacenada en la base de datos del sistema, de tal forma que en caso de reemplazo del aparato telefónico este pueda ser sustituido y la configuración de las teclas se restablezca de forma automática.
- Deberá incluir al menos 4 botones de navegación.
- 2 puertos 10/100/1000 BaseTX de switch integrado al teléfono para conexión a la red y conexión a la PC del usuario.
- Asignación de dirección IP en forma manual y mediante DHCP.
- Incluir botones para funciones de: transferencia, conferencia, colgar, último número marcado, espera, control de volumen alto y volumen bajo.
- Incluir indicador de mensaje en espera.
- Incluir botón de acceso a los mensajes de voz.
- Funciones de Jefe Secretaria.
- Acceso al directorio para realizar marcación por nombre, apellido o iniciales. El directorio deberá estar disponible para todos los teléfonos y no deberá crearse de manera individual.



CEAV
COMISION EJECUTIVA
DE ATENCION A VICTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Deberá soportar de manera preferente los Códecs de compresión G.722, G729 y G711.
- Deberá soportar QoS, 802.1p/q, DiffServ.
- Deberá contar con soporte de encriptación por medio de AES 128.
- Soporte de alimentación al teléfono mediante el cableado estructurado de datos utilizando el estándar IEEE 802.3.af, y soporte de alimentación mediante fuente de poder.
- Soporte de H323 y/o SIP.

3.3.4.6 Aparatos Telefónicos IP Semi Ejecutivos

Los teléfonos IP Semi Ejecutivos con switch integrado deben incorporar las siguientes funciones mínimas:

- Incluir pantalla de al menos cinco líneas de apariencia, a color, retroiluminada.
- Altavoz de manos libres full-duplex con cancelación de eco.
- Mínimo 10 teclas de función.
- Hasta 30 teclas programables cuya información deberá estar almacenada en la base de datos del sistema, de tal forma que en caso de reemplazo del aparato telefónico este pueda ser sustituido y la configuración de las teclas se restablezca de forma automática.
- Deberá incluir al menos 4 botones de navegación.
- Soporte de H323 y/o SIP.
- 2 puertos 10/100/1000 BaseTX de switch integrado al teléfono para conexión a la red y conexión a la PC del usuario.
- Asignación de dirección IP en forma manual y mediante DHCP.
- Incluir botones para funciones de: transferencia, conferencia, colgar, último número marcado, espera, control de volumen alto y volumen bajo.
- Incluir Indicador de mensaje en espera.
- Incluir botón de acceso a los mensajes de voz.
- Funciones de Jefe Secretaria.
- Acceso al directorio para realizar marcación por nombre, apellido o iniciales. El directorio deberá estar disponible para todos los teléfonos y no deberá crearse de manera individual.
- Deberá soportar de manera preferente los Códecs de compresión G.722, G729 y G711.
- Deberá soportar QoS, 802.1p/q, DiffServ.
- Deberá contar con soporte de encriptación por medio de AES 128.
- Soporte de alimentación al teléfono mediante el cableado estructurado de datos utilizando el estándar IEEE 802.3.af, y soporte de alimentación mediante fuente de poder.

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

3.3.4.7 Aparatos Telefónicos IP Ejecutivo

Los teléfonos IP Ejecutivo con switch integrado y capacidades de video deben incorporar las siguientes funciones mínimas:

- Pantalla táctil gráfica de al menos 7 pulgadas a color.
- Definición de 800X480 o superior.
- Dos puertos Ethernet con 10/100/1000 BT.
- Puerto de 3.5 mm para conexión de auriculares.
- Puerto HDMI que permita proyectar el contenido de video en una pantalla externa.
- Al menos un Puerto USB.
- Soporte del estándar 802.3af (PoE).
- De manera opcional brillo autoajutable según las condiciones de luz.
- Soporte de audio de banda ancha.
- Manos libres Full-duplex.
- Cancelación de eco.
- Control de Volumen y mudo.
- Cámara de video HD interconstruida.
- Contar con acceso a directorio para realizar búsqueda por nombre.
- Soporte de asignación de direccionamiento IP estático y dinámico.
- Soporte de 802.3ab LLDP-MED.
- Soporte de SNTP.
- Soporte de SIP.
- Soporte de comunicaciones de video punto a punto.
- Integración a conferencias de video con otras terminales de este tipo o softphones que lo permitan.
- Soporte de 802.1X MD5/TLS.
- Soporte de 802.1 P/Q, DSCP.

Estas terminales podrán contar con un cliente de comunicaciones unificadas (Softphone avanzado) asociado con las siguientes características:

- Servicios telefónicos. Deberá permitir generar llamadas de voz a usuarios dentro de la red de "LA CEAV" o a usuarios de la PSTN conservando sus privilegios de llamadas (LDN, Celular, etc.).
- Video llamadas y video conferencias. Deberá permitir generar llamadas de video punto a punto hacia otras terminales del mismo tipo o hacia teléfonos ejecutivos. También deberá permitir participar en conferencias multipunto con otras terminales de este tipo o aparatos telefónicos ejecutivos.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Servicios de número único y de enrutamiento de llamadas. El usuario podrá definir a partir de este cliente en donde quiere ser localizado, ya sea en el mismo cliente o en su teléfono de escritorio.
- Mensajería instantánea y presencia.
- Histórico de llamadas.
- Notificaciones: Llamadas perdidas, mensajes de voz, próximas conferencias agendadas.
- Búsqueda en el directorio (local o corporativo).
- Administración de favoritos y contactos.
- Cambio de sesión de llamada. El usuario podrá iniciar una comunicación en su terminal de escritorio y deberá contar con la opción de cambiar su llamada hacia el dispositivo en donde se tenga instalado el cliente y viceversa. El cambio deberá ser transparente para el llamante y no deberá notar este cambio de sesión ni escuchar música en espera durante el proceso.
- Este cliente deberá poder ser instalado al menos en PC y tabletas tipo IPAD.
- El cliente deberá poder conectarse a través de la red WLAN de "LA CEAV" y deberá contar con la opción de conectarse vía la red de datos celular o internet mediante un cliente VPN proporcionado por "LA CEAV".

3.3.4.8 Terminales para Audio conferencia

- Pantalla LCD 128X64 pixeles.
- Teclado alfanumérico.
- 5 botones de navegación.
- Micrófono multidireccional.
- Altavoces.
- Uso de Códecs G722, G711, G729ab.
- Uso de DTMF.
- Acceso al directorio
- Direcciónamiento DHCP e IP estático.
- Soporte de 802.1X MD5/TLS.
- Soporte de Https.
- Capacidad de grabación de las llamadas mediante un Puerto USB o mediante tarjeta SD externa.
- Gestión/calidad Del servicio.
- Soporte de 802.1 P/Q, DSCP.
- Alimentación sobre Ethernet mediante estándar IEEE 802.3af.
- Conector Ethernet RJ-45.

3.3.4.9 Aparatos Telefónicos IP Secretariales



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

Los teléfonos IP Secretariales con switch integrado deben incorporar las siguientes funciones mínimas:

- Pantalla táctil gráfica de al menos 7 pulgadas a color.
- Definición de 800X480 o superior.
- Dos puertos Ethernet con 10/100/1000 BT.
- Puerto de 3.5 mm para conexión de auriculares.
- Al menos un Puerto USB.
- Auricular alámbrico.
- Soporte del estándar 802.3af (PoE).
- Soporte de audio de banda ancha.
- Manos libres Full-duplex.
- Cancelación de eco.
- Control de Volumen y mudo.
- Contar con acceso a directorio para realizar búsqueda por nombre.
- Soporte de asignación de direccionamiento IP estático y dinámico.
- Soporte de 802.3ab LLDP-MED.
- Soporte de SNTP.
- Soporte de SIP.
- Soporte de 802.1X MD5/TLS.
- Soporte de 802.1 P/Q, DSCP.

3.3.4.10 Aparatos Telefónicos IP para Call Center

Los teléfonos IP para call center deben incorporar las siguientes funciones mínimas:

- Incluir pantalla de al menos cuatro líneas de apariencia, monocromática, retroiluminada.
- Altavoz de manos libres full-duplex con cancelación de eco.
- Mínimo 8 teclas de función.
- 2 puertos 10/100/1000 BaseTX de switch integrado al teléfono para conexión a la red y conexión a la PC del usuario.
- Asignación de dirección IP en forma manual y mediante DHCP.
- Incluir botones para funciones de: transferencia, conferencia, colgar, último número marcado, espera, control de volumen alto y volumen bajo.
- Incluir indicador de mensaje en espera.
- Incluir botón de acceso a los mensajes de voz.
- Deberá soportar de manera preferente los Códecs de compresión G.722, G799 y G711.
- Deberá soportar QoS, 802.1p/q, DiffServ.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Soporte de alimentación al teléfono mediante el cableado estructurado de datos utilizando el estándar IEEE 802.3.af, y soporte de alimentación mediante fuente de poder.
- Diadema alámbrica compatible con el equipo ofertado.

3.3.4.II Terminal IP basada en Software

Se deberán considerar teléfonos básicos basados en software (Softphones) con las siguientes funciones mínimas:

- Incluir preferentemente las mismas funcionalidades de una terminal IP Semiejecutiva.
- Servicios telefónicos. Deberá permitir generar llamadas de voz a usuarios dentro de la red de la Comisión o a usuarios de la PSTN conservando sus privilegios de llamadas (LDN, Celular, etc.).
- Compatible con Windows, OSX, IOS y android.
- Deberá permitir acceso al directorio.
- Deberá ser tarifada a través del mismo sistema ofertado sin importar el dispositivo desde el cual se use.
- Deberá pertenecer al mismo plan de numeración.
- Solución telefónica totalmente integrada al administrador de llamadas.
- Fácil integración con usuarios remotos.
- QoS Nivel 3 IP TOS/DSCP.
- G711, G729 y/o G723.1.
- Diadema alámbrica compatible con el equipo pc.

3.3.4.12 Servicios a considerar

Plan de marcación y numeración

Plan de Marcación Uniforme entre todas las extensiones del sistema (sean IP, virtuales, analógicas, por software) que incluya a todos los sitios a nivel nacional.

Directorio Telefónico Corporativo

Se debe proveer el servicio de directorio corporativo con acceso desde los teléfonos IP y softphones (Terminal IP basado en software), en todo el sistema a nivel metropolitano y nacional.

"**EL PROVEEDOR**" deberá implementar un sistema de Directorio institucional que se actualice automáticamente al modificar o ingresar un nuevo usuario telefónico con la extensión, nombre completo, puesto, inmueble, desde el conmutador a un servidor de aplicación vía web para los usuarios.

Operadora Automática



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

Los sitios principales, cuentan con el sistema de operadora automática, el cual operará de manera independiente en cada sitio, con la finalidad de controlar las llamadas telefónicas locales desde la red telefónica pública.

Consola de Operadora

Se requieren consolas de operadora para el sitio central con las siguientes características:

- Consola de Operadora basada en PC.
- Conmutación del sistema de operación estándar a un estado configurado para la actividad reducida (por la noche, por ejemplo).
- Controlar el uso de líneas internos y externos por los usuarios.
- Selección de la conexión automática de llamadas.
- Programación de la fecha y la hora del sistema, el control de los costos de las llamadas, etc.
- Teclas de función.
- Alarmas LED para indicar el status del sistema.
- Monitoreo de presencia.
- Monitoreo de extensiones en tiempo real.
- Interfaz gráfica.
- Seguridad.
- Historial.

3.3.4.13 Sistema Contact Center

"EL PROVEEDOR" deberá implementar un Centro de contacto para 20 agentes simultáneos y 1 supervisor. A continuación, se enlistan las características requeridas:

- Configuración en ambiente gráfico tipo "Drag&Drop" amigable para el usuario.
- Estadísticas y reportes.
- Posibilidad de ampliación.
- Matriz visual de supervisión y configuración.
- Estadísticas y reportes.
- CTI.
- Opción de softphone y diadema.
- Screen Pop.
- Posibilidad de administrar tráfico inbound de inicio y a futuro de outbound.

3.3.4.14 Sistema de Grabación



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Grabador integrado en la solución centro de contacto.
- Grabación simultánea de 20 llamadas de VoIP para agentes y y/o usuarios administrativos.
- Grabación de pantallas (preferentemente).
- Posibilidad de expansión para grabación de al menos 50 usuarios simultáneos.
- Deberá permitir grabación en formatos de audio WAV, MP3 y WMA.
- Deberá permitir búsqueda por fecha.

3.3.4.15 Sistema de Tarificación

Como elemento de la solución se debe ofrecer un sistema para analizar los costos de las comunicaciones y la calidad del servicio telefónico. Este sistema deberá recuperar, concentrar, consolidar y procesar la información de tarificación de los componentes de la solución como teléfonos, terminales móviles, softphones, tabletas electrónicas y smartphones.

Para la consolidación el sistema deberá proporcionar la facilidad de elaborar reportes exhaustivos e incluir una base de datos relacional donde sea posible buscar, clasificar, analizar, presentar y exportar información según criterios seleccionados provista en los CDRs del sistema.

La base de datos de este módulo deberá contener el mapa de la organización, las definiciones de informes, los CDR, los contadores de rendimiento, los libros de códigos de los operadores, así como las alarmas y eventos. La base de datos debe poderse guardar y restaurar.

Este módulo de tarificación deberá permitir manejar un entorno con varios operadores y brindar funciones de simulación que permitan efectuar la mejor elección del uso de los enlaces a la PSTN.

El sistema debe contar con la facilidad de generar reportes bajo modelos predefinidos del sistema y permitir generar formatos personalizados según las necesidades de "LA CEAV".

Dichos informes deberán poderse generar de forma automática periódicamente con la facilidad de ser enviados al administrador vía correo electrónico por el propio sistema. Estos reportes deberán poderse generar en diversos formatos como: Excel, PDF, TXT y HTML. Además de brindar mecanismos de seguridad para no mostrar números marcados que no deben ser conocidos por personas ajenas a los usuarios quienes los utilizaron.



CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

La herramienta de tarificación deberá sincronizarse con el equipo de voz, de tal forma que al crear una extensión telefónica nueva el sistema la reconozca y la procese dentro los reportes de tarificación.

Deberá ser posible generar reportes de tarificación de acuerdo a los centros de negocios establecidos por "LA CEAV".

3.3.4.16 Plan de adopción

"EL PROVEEDOR" deberá elaborar y ejecutar de manera conjunta un plan de adopción tecnológica para maximizar el uso de los sistemas de voz solicitados en el presente **Anexo I**.

3.3.4.17 Sistema de gestión y administración centralizado

El sistema de gestión y administración propuesta deberá proveer una interfaz de configuración y administración para todos los servicios y perfiles de usuario, es decir, podrán gestionarse las altas, bajas y cambios sobre usuarios desde una interfaz gráfica. Este sistema permitirá aprovisionar a los usuarios con los servicios y dispositivos necesarios con configuraciones mínimas para eficientar el tiempo de administración empleado por los administradores.

Esta aplicación de gestión deberá proporcionar como mínimo las siguientes funciones:

- Seleccionar perfiles y aplicarlos a conjuntos de usuarios.
- Definir perfiles dedicados para la creación de usuarios.
- Asociar y desasociar dispositivos a los usuarios.
- Crear y asociar en un paso nuevos dispositivos a los usuarios.
- Aprovisionamiento masivo a través de la importación y exportación de archivos tipo txt/csv.

La aplicación de administración solicitada proveerá los servicios siguientes:

- Copia de seguridad inmediata o programada para el sistema.
- Actualización de software inmediata o programada para el sistema de telefonía.
- Herramientas para el servidor de gestión y monitoreo: copia de seguridad inmediata o programada de bases de datos, desfragmentación y reinicio incluidos en el mantenimiento del servidor de gestión y monitoreo completo.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

Este módulo del sistema de gestión y administración proporcionará una interfaz de monitoreo de los componentes de la solución que mostrará indicadores de eventos, fallas y superación del umbral de rendimiento para su oportuna atención.

3.3.5 Sistema de respaldo de energía

"EL PROVEEDOR" deberá proveer el equipo necesario para soportar la carga generada por el equipo tanto de telefonía IP, Red LAN y Seguridad Lógica. A continuación, se describen las características mínimas con las que deben cumplir los equipos ofertados:

Sistema de UPS Interactivo de 1500VA para equipos de servidores, redes y telecomunicaciones.

El equipo debe contar mínimo con las siguientes características:

- a) Requiere sólo 2 espacios de rack (2U).
- b) Ofrecer 21 minutos de funcionamiento autónomo con media carga y 7,5 minutos mínimos con carga completa.
- c) El funcionamiento se puede expandir con módulos de baterías externas opcionales.
- d) Debe mantener regulada la salida nominal de 120V sin utilizar la energía de la batería durante las caídas tensión y sobretensiones de 83 a 145V.
- e) Debe incluir al menos un total de 8 tomacorrientes con 2 bancos de carga que se pueden controlar individualmente mediante la interfaz del software para reiniciar equipos seleccionados a pedido o que eliminen cargas menos significativas para ampliar el funcionamiento de la batería para más equipos vitales.
- f) Soporta el monitoreo remoto del UPS y de las condiciones eléctricas del lugar mediante los puertos de monitoreo USB y DB9 incorporados.
- g) Se requiere que incluya software de monitoreo y apagado autónomo del UPS con cableado completo.
- h) Debe de contar de manera interna o agregando un accesorio que permita soportar SNMP.
- i) Se requiere que tenga una interfaz de apagado de emergencia que ofrezca la opción de apagado instantáneo del UPS y del equipo conectado en caso de incendio o emergencia.
- j) Debe contar con alarmas sonoras multifunción e indicadores visuales en el panel que permitan conocer a simple vista el estado del UPS y de la energía de la línea.
- k) La supresión de sobretensiones de CA de grado de red protege a los equipos de daños y problemas de funcionamiento causados por sobretensiones transitorias y ruidos en la línea.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- l)** Entrada: NEMA 5-15P / Salida: 8 NEMA 5-15R (120V). Si la ubicación no cuenta con este tipo de entrada se deberá contemplar la instalación de esta.

Se debe de considerar el equipo de montaje para la instalación en un rack de 20U mínimo tipo gabinete

Sistema de UPS interactivo de 3000VA para equipos de servidores, redes y telecomunicaciones

- a)** Para montar en rack 2U.
- b)** Ofrecer una carga de 2250Watts que nos de 3.5 minutos y a media carga 1125Watts 10 minutos.
- c)** El funcionamiento se puede expandir con módulos de baterías externas opcionales.
- d)** Debe contar con regulación automática de voltaje manteniendo la salida nominal regulada de 100/110 y 120V sin utilizar energía de la batería durante caídas de voltaje y sobre voltajes de 83 volts hasta 145 volts.
- e)** Soporte el monitoreo remoto del UPS y de las condiciones eléctricas del lugar mediante los puertos de monitoreo USB y DB9 incorporados.
- f)** Se requiere que incluya software de monitoreo y apagado autónomo del UPS con cableado completo.
- g)** Debe de contar de manera interna o agregando un accesorio que permita soportar SNMP
- h)** Se requiere que tenga una interfaz de apagado de emergencia que ofrezca la opción de apagado instantáneo del UPS y del equipo conectado en caso de incendio o emergencia.
- i)** Debe contar con alarmas sonoras multifunción e indicadores visuales en el panel que permitan conocer a simple vista el estado del UPS y de la energía de la línea.
- j)** Entrada: NEMA 5I-30P (120V 30^a) / Salida: 1 L5-30R, 8 NEMA 5-15/20R (120V). Si la ubicación no cuenta con este tipo de entrada se deberá contemplar la instalación de esta.

Se debe de considerar el equipo de montaje para la instalación en un rack de 20U mínimo tipo gabinete.

Sistema de UPS interactivo de 5000VA para equipos de servidores, redes y telecomunicaciones

- a)** Para montar en rack 6U.
- b)** Ofrecer 38 minutos de funcionamiento autónomo con media carga mínimo y 15 minutos mínimos con carga completa.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- c) El funcionamiento se puede expandir con módulos de baterías externas opcionales.
- d) Debe contar con regulación automática de voltaje manteniendo la salida nominal regulada de 208V y 120V sin utilizar energía de la batería durante caídas de voltaje y sobre voltajes de 151 volts hasta 282 volts.
- e) Soporte el monitoreo remoto del UPS y de las condiciones eléctricas del lugar mediante los puertos de monitoreo USB y DB9 incorporados.
- f) Se requiere que incluya software de monitoreo y apagado autónomo del UPS con cableado completo.
- g) Debe de contar de manera interna o agregando un accesorio que permita soportar SNMP
- h) Se requiere que tenga una interfaz de apagado de emergencia que ofrezca la opción de apagado instantáneo del UPS y del equipo conectado en caso de incendio o emergencia.
- i) Debe contar con alarmas sonoras multifunción e indicadores visuales en el panel que permitan conocer a simple vista el estado del UPS y de la energía de la línea.
- j) Entrada: NEMA L6-30P (208V 30") / Salida: 1 L6-30R, 1 L14-30R, 10 NEMA 5-15(120V), 2 NEMA 5-20R (208V). Si la ubicación no cuenta con este tipo de entrada se deberá contemplar la instalación de esta.

Se debe de considerar el equipo de montaje para la instalación en un rack de 20U mínimo tipo gabinete.

3.3.6 Gabinete para montaje de los equipos (Rack)

Como complemento para el Sistema de Telefonía y el Equipamiento LAN, "EL PROVEEDOR" deberá considerar los siguientes gabinetes.

Sitio Central Gabinete de 40U, por 36" de profundidad mínimo.

A continuación, se describen los requerimientos mínimos que debe cumplir el gabinete:

- Estructura de acero.
- Puerta frontal y trasera de acero de rejilla con cerraduras de seguridad y desmontables.
- Costados desmontables con cerraduras de seguridad.
- Ranuras de ventilación en la parte inferior y superior del gabinete las cuales permiten un adecuado flujo de aire.
- Sistema de montaje y fijación a piso falso.
- Cuatro patas niveladoras.
- Techo preparado para fijar hasta cuatro ventiladores.



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Lámpara de luz de 15 watts.
- Unidades de rack: 40 UR.
- Sistemas de fijación en rack: Tuerca enjaulada M6.
- Profundidad: 36" mínimo.
- Barra de cobre.
- Dos camas de cableado de piso a techo del gabinete para amarre de cables.
- Sistema de ventilación integrado.
- Sistema de monitor y teclado para gabinete con las siguientes características:
 - Sistema KVM analógico.
 - Teclado/mouse USB, video VGA.
 - Pantalla plana deslizable.
 - 1 UR.
 - Conectividad TCP/IP.
 - Rieles estáticos.

Sitio Remoto Gabinete de 20U, por 36" de profundidad mínimo.

A continuación, se describen los requerimientos mínimos que debe cumplir el gabinete:

- Estructura de acero.
- Puerta frontal y trasera de acero de rejilla con cerraduras de seguridad y desmontables.
- Costados desmontables con cerraduras de seguridad.
- Ranuras de ventilación en la parte inferior y superior del gabinete las cuales permiten un adecuado flujo de aire.
- Sistema de montaje y fijación a piso falso.
- Cuatro patas niveladoras.
- Techo preparado para fijar hasta cuatro ventiladores.
- Lámpara de luz de 15 watts.
- Unidades de rack: 20 UR.
- Sistemas de fijación en rack: Tuerca enjaulada M6.
- Profundidad: 36" mínimo.
- Barra de cobre.
- Dos camas de cableado de piso a techo del gabinete para amarre de cables.
- Sistema de ventilación integrado.

3.3.7 Sistema de Monitoreo de desempeño de los componentes de red



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

Esta herramienta será para uso exclusivo de "LA CEAV" y será independiente a los sistemas que "EL PROVEEDOR" deberá proporcionar en los servicios de Mesa de Ayuda y NOC. "EL PROVEEDOR" deberá proporcionar el equipamiento necesario para el monitoreo de 150 elementos de red como mínimo.

Las herramientas que se integren no deberán ser software libre o de dominio público y deberán contar con el soporte vigente del fabricante.

Adicionalmente las herramientas deberán proveer información sobre la capacidad de los equipos, tanto en su presentación visual, como de los reportes, notificaciones y la emisión de informes del rendimiento que sean generados.

La herramienta debe de considerar, al menos, las siguientes tareas de gestión y monitoreo:

- a) Deberá proveer al menos las siguientes métricas de utilización y desempeño, las cuales serán incluidas en los reportes.
 - Disponibilidad de cada dispositivo.
 - Utilización de CPU.
 - Utilización de memoria.
 - Utilización de ancho de banda.
 - Latencia.
 - Paquetes perdidos.
 - Throughput total de cada dispositivo.

El monitoreo deberá tener la capacidad de ajustar el tiempo de poleo de cada una de las métricas colectadas.

El monitoreo deberá contar con una interfaz en la que se puedan visualizar de forma gráfica las métricas monitoreadas por cada dispositivo.

Las lecturas deberán poder actualizarse en línea y deberán contar con la facilidad de generar mediante filtros: reportes que representen informes del comportamiento de la red por días, semanas, meses.

La herramienta de monitoreo deberá ser capaz de monitorear equipos a través de los siguientes protocolos: SNMP v1, v2, v3 e ICMP.

La herramienta deberá ser capaz de descubrir automáticamente todos los elementos de red que tengan una dirección IP con la finalidad de obtener un inventario de la infraestructura instalada.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

Deberá permitir configurar umbrales por cada elemento y variable monitoreada en cada uno de los dispositivos.

La herramienta de monitoreo deberá contar con la capacidad de graficar métricas de disponibilidad, utilización y desempeño, en las siguientes escalas: diarias, semanal, mensual.

La información de la base de datos de la solución de monitoreo deberá de contar con la capacidad de ser exportada parcial en su totalidad a otro tipo de motor de base de datos comercial, ej. MS SQL SERVER.

Consola única para monitoreo de punta a punta (red, infraestructura, aplicaciones, transacciones y usuarios).

Monitoreo con o sin agente.

Umbrales dinámicos y estáticos para crear un baseline dinámico.

Log Monitoring integrado y automatizado asociado a eventos.

Correlación de eventos.

Pintado de servicio (y sus dependencias) impactados.

Integración nativa a mesa de ayuda para levantar tickets automáticos e inteligentes.

Flujos de remediación automática.

CMDB incluida.

3.4 Soporte y monitoreo

3.4.1 Centro de Operaciones de Red (NOC)

"**EL PROVEEDOR**" deberá ofrecer un soporte técnico de primer y segundo, a través de un centro de operaciones de Red NOC (Network Operation Center) para ofrecer el servicio de Monitoreo Remoto de Redes. Los incidentes relacionados con el servicio serán reportados a través de la mesa de ayuda "**EL PROVEEDOR**" por cualquiera de los métodos y niveles jerárquicos de escalación establecidos por el mismo.

Este servicio deberá operar las 24 horas del día, los 7 días de la semana y asistencia en español, a fin de vigilar la operación de la Infraestructura de comunicaciones solicitada en el presente alcance por "**LA CEAV**".



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

La disponibilidad del soporte telefónico deberá ser de 24 horas, los 365 días del año y en español, contando con un esquema de escalación de al menos dos niveles jerárquicos superiores (de conocimiento y toma de decisión) que serán requeridos y escalonados después de 2 horas, durante las cuales no se haya finalizado el reporte.

"EL PROVEEDOR" deberá proporcionar los nombres, cargos, teléfonos fijos y celulares del personal destinado a la atención telefónica para el soporte. Además de los procedimientos de generación de tickets con el que se operará el servicio.

Los aspectos que contemplar para el monitoreo de redes son los siguientes:

- a) Monitoreo en tiempo real desde el NOC **"EL PROVEEDOR"** hasta los sitios que integran la infraestructura de **"LA CEAV"**.
- b) Identificación de umbrales de operación normales para contar con referencias adecuadas para la detección de tendencias y/o problemas que puedan afectar el funcionamiento de la red.
- c) Análisis continuo de tendencias operativas que permita contar con parámetros de mejora en la infraestructura de red.
- d) Emisión de alarmas en caso de sobrepasar los umbrales normales de operación y avisos al personal especializado a través de mensajes SMS y/o correo electrónico.

Dentro de los servicios del NOC se requiere que existan herramientas con las siguientes características de gestión y monitoreo de los appliance UTM:

3.4.1.1 Sistema de reporte, análisis y almacenamiento de bitácoras

Sistema de reporte, análisis y almacenamiento de bitácoras, que incluye capacidades de correlación y análisis de vulnerabilidades en la red para dispositivos de Administración Unificada de Amenazas (UTM por sus siglas en inglés, Unified Threat Management).

Generalidades

- Formato tipo appliance (dispositivo de propósito específico).
- Sistema operativo propietario.
- Interface de administración gráfica (GUI) vía Web (http y HTTPS).
- Interface de administración vía CLI (Línea de comando) vía telnet, ssh y consola serial.
- Debe tener la posibilidad de definir administradores para la solución, de modo que pueda segmentarse la responsabilidad de los administradores por tareas operativas.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA

- Debe tener la capacidad de poder integrar dispositivos tipo UTM para que le reporten, y establecer comunicaciones seguras con dichos dispositivos.
- Debe tener la capacidad de asignar cuotas de espacio en disco por dispositivo, de modo que un solo dispositivo no consuma la totalidad del disco de la solución.
- Debe consolidar en el dispositivo.

Análisis Forense y Correlación

- Debe ser capaz de hacer correlación de la información almacenada. Esto es, identificar patrones y/o tendencias en la información almacenada.
- Debe de ser capaz de hacer búsquedas por username o dirección IP, para que toda la información almacenada de dicho username o dirección IP sea mostrada en un reporte donde pueda darse seguimiento a su actividad.

Análisis de vulnerabilidades

- Debe poseer (integrado o por separado) la capacidad de hacer análisis de vulnerabilidades en la red, mediante plug-ins de ataques actualizables, y generar un reporte de cuáles vulnerabilidades fueron encontradas en la red.

Cuarentenas

- Debe de poder recibir archivos de dispositivos o mecanismos antivirus compatibles con la finalidad de usar el espacio en disco como espacio para cuarentena.
- Debe de poder recibir archivos de dispositivos o mecanismos antispam compatibles con la finalidad de usar el espacio en disco como espacio para cuarentena.

Almacenamiento de Contenido

- Debe ser capaz de recibir bitácoras de los protocolos http, SMTP y messengers (Yahoo, MSN) para poder almacenar los mensajes que han fluído en la red a través de dichos protocolos, para su posterior visualización.
- Los mensajes deberán poder ser almacenados completamente, o solo un "resumen" de la conexión. El mensaje completo exhibirá el contenido completo, mientras que el resumen solo mostrará fuente y destino de la comunicación, así como su duración.
- Debe de ser capaz de hacer búsquedas sobre los mensajes almacenados.

Licenciamiento



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFÓNIA"

- Capacidad de administrar al menos 30 dispositivos iniciales.
- Vigencia de licencia de actualización. El equipo debe de incluir Soporte Telefónico 24x7, reemplazo de fábrica y actualizaciones de firmware.

Desempeño y conectividad

- Capacidad mínima de almacenamiento incluida: 1Tb.
- Conectividad con interfaces Ethernet 10/100/1000: 4.
- Dispositivos UTM que pueden enviar bitácoras: 150.
- La plataforma se prefiere en un solo dispositivo "appliance". Sin embargo, es posible entregarlo en una plataforma de varios servidores de propósito específico. No se aceptan dispositivos de propósito genérico y/o con sistemas operativos genéricos.

3.4.1.2 Consola de administración centralizada para dispositivos de seguridad tipo UTM

Sistema de gerenciamiento (consola de administración) centralizado que realiza provisiónamiento basado en políticas, configuración de dispositivos, gerenciamiento de actualizaciones, monitoreo y control de dispositivos de seguridad que sean del tipo "Gerenciamiento Unificado de Amenazas" (Unified Threat Management).

Generalidades

- Centralización de Configuración y monitoreo de todos los dispositivos de seguridad UTM. Así como todas sus funciones de protección de red.
- Por seguridad y eficiencia, debe ser un "appliance" de propósito específico para el gerenciamiento de la seguridad. No se aceptan plataformas basadas en sistemas operativos genéricos y/o hardware genérico.
- Se incluye la administración de dispositivos "virtuales" que residen en una misma unidad física. Estos equipos virtuales pueden ser administrados como un dispositivo completamente independiente dentro de la consola, con su propia configuración y administración. Esta capacidad permite consolidar en el número menor posible de consolas, preferentemente una, la administración de las diversas funcionalidades de protección completa de contenido.
- Creación, almacenamiento e implementación automatizada de configuraciones de dispositivos.
- Permitir tener un solo repositorio de almacenamiento centralizado y administración de configuraciones, para simplificar las tareas de administración de una gran cantidad de dispositivos de seguridad con protección completa de contenido.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- Las comunicaciones entre la consola de administración y los dispositivos administrados deben ser cifradas (Encriptadas).
- La interface de administración es basada en Web Seguro (HTTPS).
- Para un eficiente almacenamiento de las configuraciones, debe incluirse una base de datos relacional integrada compatible con la solución.
- Administración basada en roles para permitir a los administradores delegar los derechos a dispositivos específicos con los privilegios adecuados de lectura/escritura.
- Configuración basada en scripts para una mejor flexibilidad y control. Esta funcionalidad permite la automatización de tareas operativas, cuya implementación puede ser de forma masiva, con tiempos de aplicación mínimos a los dispositivos administrados.
- Se debe poder realizar automatización calendarizada de respaldos de la configuración y las bitácoras.
- Se debe poder realizar operaciones sobre grupos de dispositivos, y añadir/cambiar/borrar dispositivos de esos grupos.
- Permitir el hospedaje local de actualizaciones de firmas de AV / IPS y filtrado de contenido web y Antispam, de los dispositivos UTM. Esto permite el almacenamiento de forma local de las bases de datos de protección AV e IPS, además de Filtrado de Contenido y Anti-SPAM, con la finalidad de disminuir el tráfico de consultas de actualizaciones a Internet a lo mínimo, evitando el consumo innecesario de ancho de banda, permitiendo la utilización de este para los fines requeridos por los usuarios de red.
- Contiene un administrador de Software UTM de Escritorio que permite la consolidación de las consolas de seguridad informática en el menor número posible de dispositivos, con el ideal de reducirlo a uno, disminuyendo al mínimo las tareas de operación de diferentes tecnologías en diferentes equipos.
- La administración de software de escritorio posibilita la administración de la funcionalidad de Antivirus, Anti-SPAM, Firewall para host, Anti-Spyware, Cliente de VPN IPSEC y Filtrado de contenido para el PC. Todo desde la misma consola de administración, para permitir el aseguramiento y aplicación de políticas de seguridad y contenido desde un solo punto de administración.
- Mediante una conexión a un dispositivo externo de almacenamiento y procesamiento de bitácoras en tiempo real, el dispositivo de administración puede solicitar reportes en línea, con una interfaz de administración completamente integrada. Esto permite descargar las tareas de pre-procesamiento de bitácoras y reportes en un segundo dispositivo dedicado a esta tarea, de manera que se eficientiza la utilización de recursos de la consola de administración.
- Capacidad de crear, exportar y almacenar versiones de configuración de los dispositivos administrados, antes de aplicar cambios a un dispositivo.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

De esta forma, se disminuye la posibilidad de cometer un error no intencional al modificar una política y permite regresar a una configuración en un estado operacional después de haber aplicado una implementación con resultados no esperados.

- Incluye un subsistema Monitoreo en Tiempo-Real. Esto permite al equipo de monitoreo y administración obtener el estado actual de la infraestructura de dispositivos administrados, y permitir actuar proactivamente a un evento de seguridad y operación de los dispositivos de seguridad administrados.
- Posibilidad de administrar el firmware de los dispositivos de seguridad, permitiendo programar y aplicar actualizaciones de sistema operativo de forma desatendida a un equipo o grupo de equipos administrados por la consola, reduciendo tiempos de operación y administración del personal que administra los equipos de seguridad.
- La consola de administración permite configuración en Alta Disponibilidad, de tal forma que en caso de falla pueda existir otro equipo en línea que tome las tareas del equipo dañado con una pérdida mínima en la disponibilidad del servicio.
- Capacidad de creación y aplicación de configuraciones de VPN entre los dispositivos de seguridad administrados.
- Subsistema de monitoreo especial para los túneles de VPN de tal forma que el área de operación puede monitorear desde una sola pantalla el estado de todos los túneles de VPN establecidos, administrados y operados desde la consola de administración.
- Debe soportar al menos 30 modelos diferentes de dispositivos UTM.

Licenciamiento

- Capacidad de administrar al menos 30 dispositivos iniciales.
- Vigencia de licencia de actualización. El equipo debe de incluir Soporte Telefónico 24x7, reemplazo de fábrica y actualizaciones de firmware.

Desempeño y conectividad

- Interfaces Ethernet 10/100/1000 Mbps: 4.
- Debe incluirse conexión por consola serial (puerto serial) al equipo con cables de conexión incluidos.
- Dispositivos tipo UTM administrados: 30.
- Capacidad de disco duro (almacenamiento) incluido: Al menos 1TB.
- La plataforma se prefiere en un solo dispositivo "appliance". Sin embargo, es posible entregarlo en una plataforma de varios servidores de propósito específico. No se aceptan dispositivos de propósito genérico y/o con sistemas operativos genéricos.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

3.4.2 Mesa de Servicios

"**EL PROVEEDOR**" ofrecerá una Mesa de Servicio con atención 7x24 durante la vigencia del contrato, que será el punto de contacto único con "**LA CEAV**", en el cual se recibirán las solicitudes de "**LA CEAV**".

La Mesa de Servicio estará a cargo de la operación de los servicios solicitados en el presente **Anexo I** teniendo como tareas lo siguiente:

- i. Identificar las posibles actualizaciones o mejoras a la misma, para efectos de que sean incluidas al programa de aprovisionamiento de la infraestructura tecnológica.
- ii. Elaborar un programa de mantenimiento de la infraestructura tecnológica que contenga acciones de carácter preventivo para evitar fallas a los componentes de dicha infraestructura.
- iii. Aplicar los controles de mitigación de riesgos establecidos en la seguridad perimetral.
- iv. Modificar, en los componentes instalados, las contraseñas originales, configuraciones y parámetros que puedan afectar la seguridad y suprimir los accesos temporales utilizados en la instalación.
- v. Coordinar al menos un mantenimiento preventivo durante el periodo del contrato, a todas las tecnologías que conforman la propuesta técnica, y aplicará el servicio correctivo sin límite de eventos.
- vi. Registrar y dar seguimiento a los incidentes de mantenimiento, con el propósito de analizar y eliminar las vulnerabilidades dentro de la infraestructura tecnológica.
- vii. Llevar la administración del inventario tanto de altas, bajas y cambios de todos los equipos.

Se deberá indicar en su propuesta técnica, la matriz de escalación, la cual contendrá al menos la información de los contactos (Nombre, Puesto, Teléfono Oficina, Teléfono Móvil, etc.) para su localización en todo momento, así como los tiempos establecidos para pasar al siguiente nivel.

"**LA CEAV**" proporcionará una matriz de escalación de contactos y responsables a fin de coordinar la restauración de los servicios a "**EL PROVEEDOR**".

La Mesa de Servicio deberá realizar las Altas, Bajas y Cambios de los servicios en dos formas:

1. Derivado de migraciones en hardware o software "**EL PROVEEDOR**" requiera hacer cambios, estos serán reportados a "**LA CEAV**" con al menos 48 hrs. de anticipación previo a su autorización.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

2. Cuando **"LA CEAV"**, solicite una Alta, Baja o Cambio, **"EL PROVEEDOR"** clasificará el requerimiento, analizará el impacto en la infraestructura actual y definirá su viabilidad, la cual será comunicada a **"LA CEAV"** junto con su fundamento para poder tomar una decisión.

Una vez autorizado se realizará el alta, baja o cambio solicitado, procederá a realizar el alta, baja o modificación de los servicios o infraestructura, se realizará Pruebas de Operación y dará de alta el nuevo servicio en el sistema de administración y monitoreo, Actualizará las bases de datos y memorias técnicas.

En caso de altas, bajas o cambios requeridos de inmediato, se solicitarán vía correo electrónico o por teléfono y se determinará si se realizarán de manera remota o en sitio, pudiendo tener la opción de ir dando indicaciones al contacto en sitio en caso de cambios menores.

La Mesa de Servicio generará y mantendrá actualizada una memoria técnica de los servicios integrando los correspondientes controles de cambios.

Evento	Tiempo máximo de registro del reporte	Tiempo máximo de Solución
Solicitudes relacionadas con Altas, Bajas y Cambios de los servicios y configuraciones en operación	10 minutos	2 días naturales
Solicitudes de implementación de servicios adicionales (Cambios de Domicilios)		2 semanas
Solicitudes de implementación de servicios adicionales (Crecimiento y Nuevos Sitios)		4 semanas

3.4.3 Mantenimiento correctivo

"EL PROVEEDOR" mantendrá operando y en servicio los equipos y deberá de considerar que en caso de falla deberá sustituir los equipos por otros dispositivos de igual o superiores características que permita mantener la red estable.

"EL PROVEEDOR" realizará los mantenimientos correctivos necesarios acorde a los tiempos de respuesta mencionados en la tabla de atención y solución de incidentes y tiempos de respuesta (4. Niveles de Servicio).

En todos los casos, la respuesta en sitio y el envío de refacciones serán en la oficina central y/o sitios remotos.

Consideración.

"EL PROVEEDOR" deberá entregar una carta de cada una de las tecnologías solicitadas emitida por el fabricante y firmada por representante legal del mismo en donde manifieste que se compromete a cumplir con los niveles de servicio solicitados en el presente **Anexo I**.

3.4.4 Mantenimiento preventivo

"EL PROVEEDOR" realizará al menos un mantenimiento preventivo de acuerdo con las necesidades de cada uno de los equipos asociados al servicio, contabilizados a partir de la fecha de la entrega de éstos.

Deberán implementar los procedimientos y mecanismos, así como prever y considerar el equipo, refacciones, materiales, insumos y personal especializado necesario para llevar a cabo las labores de mantenimiento de la infraestructura total que se utilice para proporcionar el servicio objeto de esta licitación, sin que esto genere un costo adicional para la convocante. El servicio deberá incluir de forma enunciativa más no limitativa los siguientes puntos:

- Plan de trabajo aprobado por **"LA CEAV"**.
- Respaldo de configuraciones de los equipos entregado en forma electrónica a **"LA CEAV"**.
- Control de cambios de firmware (manejo de un repositorio de firmware, revisión de recomendaciones de fabricante para la actualización de estos, actualización en los equipos).
- Identificación de cables de parcheo conectados al switch (mantener el mismo orden antes y después del mantenimiento).
- Limpieza de gabinetes.
- Sopleteado y aspirado de los componentes.
- Memoria técnica.
- Descripción de las actividades realizadas.
- Fotografías de los equipos antes y después del mantenimiento.
- Observaciones y recomendaciones de las condiciones del equipo.
- A la conclusión de cada servicio de mantenimiento preventivo y/o correctivo, se elaborará un reporte que contenga tanto las actividades realizadas, el estado que guardan los equipos y deberá incluir la fecha y horario de inicio y terminación del reporte.
- Los técnicos de servicio asignados por **"EL PROVEEDOR"** deberá contar con equipos de cómputo personal y medio de comunicación (teléfono celular) para que puedan estar localizados en el tiempo de servicio durante la vigencia del contrato.



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

El servicio de mantenimiento preventivo ofertado deberá incluir refacciones y mano de obra, así como la limpieza de los equipos, por lo que **"EL PROVEEDOR"** debe contar con la infraestructura necesaria que les permita proporcionar este servicio.

Descripción de los servicios que incluye el mantenimiento preventivo.

Actividades previas

- Medición de voltajes en rack de comunicaciones.
- Verificación de voltajes e inducción en tierra física.
- Verificación del hardware (tarjetas y módulo) y software (programación y versión que tiene el equipo) instalado en el equipo a través de una pc antes de la limpieza.
- Acomodo y amarre del cableado.

Actividades de limpieza

- Extracción del polvo en equipo de comunicaciones.
- Sistema de Monitoreo de desempeño de los componentes de red.
- Limpieza de gabinetes de equipo de comunicaciones con cremas y líquidos limpiadores no corrosivos.

Actividades de verificación

- Realización de pruebas del correcto funcionamiento de los equipos mediante software y hardware especializado y las facilidades que el mismo equipo tiene para este fin realizando rutinas de prueba.
- Recolección de la información de configuración de los equipos, memoria, puertos y verificar el correcto funcionamiento del procesador después del servicio de limpieza.

Actividades de reporte

- Reporte de mediciones iniciales y finales.
- Reporte de anomalías detectadas.
- Actualización de bitácoras de servicio.
- Se entregará una copia de cada uno de los reportes al personal designado por **"LA CEAV"**.

En todos los casos, la respuesta en sitio y el envío de refacciones serán en la oficina central y/o sitios remotos.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

3.4.5 Garantía

- 1) Para todo el equipamiento de la solución, la garantía será la vigencia del contrato en todas sus partes, considerando mano de obra, configuración y componentes sin costo adicional.
- 2) La garantía de la solución se brindará en sitio.

La garantía de la solución se brindará en sitio.

3.5 Transición

3.5.1 Transición Inicial

La instalación de los equipos deberá estar completada a más tardar un día natural previo al inicio de la vigencia del servicio.

En caso de que al inicio de la vigencia del servicio **"EL PROVEEDOR"** no cuente con la totalidad de los equipos ofertados, podrá entregar e instalar equipos de similares características, por un periodo máximo de 31 días naturales a partir del plazo señalado.

Los equipos entregados a partir del inicio de la vigencia que caigan en el supuesto anterior no serán sujetos de deductivas, siempre y cuando sean de características similares, la validación será realizada por la Dirección de Tecnologías de la Información, por los que se pagará la parte proporcional de los días de operación del equipo, tomando como base el 50% del costo mensual del equipo ofertado.

La entrega, instalación y configuración de los equipos ofertados deberá estar terminada a más tardar el 20 de enero de 2020; en caso de que para las 00:00 horas del 21 de enero de 2020, no se cuente con los mismos, se aplicarán las penas convencionales y/o deducciones correspondientes.

"EL PROVEEDOR" deberá contemplar dentro de su plan de trabajo que **"LA CEAV"** no cuenta con bodega para resguardo de los equipos.

3.5.2 Transición Final

Al término de la vigencia del contrato, **"EL PROVEEDOR"** estará obligado a realizar las actividades propias de transferencia y migración de los servicios hacia un nuevo proveedor de servicios, a partir de que se le notifique por parte del área requirente dentro de la vigencia del contrato.



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

Deberá disponer del personal necesario para coordinar la transferencia integral del servicio con el futuro proveedor del servicio, elaborando conjuntamente la logística de transición, misma que será avalada y autorizada por la Dirección de Tecnologías de la Información.

Al final de la etapa de migración de servicios, **"EL PROVEEDOR"**, retirará toda la infraestructura y servicios que hubieran sido parte de la solución y que sean única y exclusivamente de su propiedad.

"EL PROVEEDOR" deberá considerar que mantendrá en funcionamiento de toda la infraestructura por un periodo de tiempo máximo de 1 mes para que se pueda realizar las actividades de transición gradualmente y así mantener la continuidad del servicio. Dicho periodo será proporcionado sin costo adicional.

3.6 Servicios Adicionales

3.6.1 Cambios de domicilio

"EL PROVEEDOR" deberá considerar como parte de la propuesta hasta 5 cambios de domicilio sin costo para **"LA CEAV"**.

Los costos de desinstalación, transporte e instalación en el nuevo sitio deberán estar incluidos en el contrato.

En caso de exceder el número de cambios previstos, el costo será el señalado en el Catálogo de Servicios **Apéndice I**.

"LA CEAV" garantizará que las condiciones de los nuevos inmuebles estarán listas antes de la instalación, será responsabilidad de **"LA CEAV"** proveer energía eléctrica, cableado, tierras, clima y espacios para dicho propósito.

En caso de requerirse cambios de domicilio **"CEAV"** avisará a **"EL PROVEEDOR"** adjudicado del servicio con 15 días naturales de anticipación con el fin de planear las fechas, materiales y logística. A partir de la fecha de notificación de **"LA CEAV"**, **"EL PROVEEDOR"** tendrá 2 semanas para la entrega del servicio los cuales se darán por recibidos con una carta de entrega y el costo y se incluirá en la factura posterior en el caso de aplicar.

3.6.2 Equipo Adicional

"LA CEAV" podrá solicitar el incremento de equipos y/o servicios señalados en el **Apéndice I** Catálogo de Servicios.



CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

El costo del equipamiento adicional será el establecido en el Catálogo de Servicios (**Apéndice I**).

"**LA CEAV**" formalizará mediante un oficio dicho incremento, el proveedor contará con 30 días naturales máximo para la entrega, configuración y puesta en marcha.

"**EL PROVEEDOR**" deberá entregar los equipos y/o servicios en un máximo de 30 días naturales para la entrega, instalación y configuración de los equipos adicionales.

3.6.3 Nuevos Sitios

Los nuevos sitios se refieren a proveer el equipamiento necesario y/o servicios para cubrir las necesidades que así lo requiera "**LA CEAV**".

El costo del equipamiento adicional será el establecido en el Catálogo de Servicios (**Apéndice I**).

En caso de requerirse nuevos sitios, "**LA CEAV**" solicitará de manera formal la cotización de dichos servicios.

"**EL PROVEEDOR**" deberá entregar los equipos y/o servicios en un máximo de 30 días naturales para la entrega, instalación y configuración de los equipos adicionales.

4. Niveles de "EL SERVICIO"

"**EL PROVEEDOR**" deberá contar con personal encargado de dar seguimiento a incidentes que afecten los servicios de la infraestructura de red de "**LA CEAV**".

"**EL PROVEEDOR**" deberá contar con los siguientes tiempos de atención y solución para el cumplimiento de los niveles de servicio requeridos por "**LA CEAV**".



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

Niveles de Atención y Solución para el Sitio CENTRAL (Ciudad de México)	
Tiempo Máximo de Atención.	10 minutos para eventos que afectan problemas de alta importancia, caída de equipos centrales o controladoras y/o pérdida de comunicación con 25% o más de los enlaces asociados al equipo con la falla. 2 horas para problemas que afectan a una sola área o departamento 8 horas si se trata de problemas que afectan a un usuario en particular y no tienen impacto sobre los departamentos y/o áreas críticas dentro de la red. También están incluidos requerimientos generales, requerimientos de instalación, movimientos, adición o cambios en los equipos y/o aplicaciones de la red (en caso de tener la responsabilidad de operación de aplicaciones)
Tiempo de solución de la falla.	4 horas para eventos que afectan problemas de alta importancia, caídas de equipos centrales o controladoras y/o pérdida de comunicación con 25% o más de los enlaces asociados al equipo con la falla. 12 horas para problemáticas que afectan una sola área o departamento y que no afectan los procesos centrales de funcionamiento. 24 horas si se trata de problemas que afectan a un usuario en particular y no tienen impacto sobre los departamentos y/o áreas críticas dentro de la red. También están incluidos requerimientos generales, requerimientos de instalación, movimientos, adición o cambios en los equipos y/o aplicaciones de la red (en caso de tener la responsabilidad de operación de aplicaciones).

Niveles de Atención y Solución para el Sitios Remotos (Interior de la República)

Cambios de Domicilio

Niveles de atención y solución	
Tiempo máximo de atención.	2 días para entregar cotización de dicho cambio de Domicilio.
Tiempo de solución	2 semanas a partir de que se confirma mediante oficio dicho cambio.



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

Equipo adicional

Niveles de atención y solución	
Tiempo máximo de atención.	2 días para entregar cotización de dicho cambio de Domicilio.
Tiempo de entrega	30 días naturales a partir de que se confirma mediante oficio dicho incremento.

Nuevos sitios

Niveles de atención y solución	
Tiempo máximo de atención.	2 días para entregar cotización de dicho cambio de Domicilio.
Tiempo de entrega	30 días naturales a partir de que se confirma mediante oficio dicho incremento.

Disponibilidad del servicio por equipos

Para el Switch Core, Firewall UTM Tipo A y B, Teléfonos IP Básicos, Semi Ejecutivo, Secretarial, Call Center, Basada en Software, Terminal Audio Conferencia y Gateway Central así como Remoto y Sistemas de Administrador de Llamadas, Telefonía IP, Call Center, Grabación y Tarificación disponibilidad mensual del 99.5%

Para Switches de Acceso Tipo A y B, Controlador de Wireless y Puntos de Acceso, disponibilidad mensual del 99.2%

Para Consolas de Monitoreo y Operadora, disponibilidad mensual del 99.0%

% Disponibilidad = $(1 - (HF_s / H_t)) \times 100$

HF_s = Acumulado de horas transcurridas fuera de servicio durante el mes.
(Se toma la hora de inicio del reporte con la que se levantó hasta la hora del cierre de este.)

H_t = Número total de horas del mes.
(Número Total de Horas en el mes = 30 días x 24 horas total 720 hrs.)

5. Confidencialidad

"EL PROVEEDOR" y su personal, no harán uso indebido de la información, documentación ni activos a los que, con motivo de la prestación de "EL



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

SERVICIO" tenga acceso, así como aquellos que se generen con motivo de la prestación de este, en el entendido de que en caso contrario se procederá conforme a derecho por los daños o perjuicios que causen a **"LA CEAV"** el uso, duplicado, reproducción, publicación de documentación oficial que se llegaren a realizar.

6. Entregables

"EL PROVEEDOR" deberá cumplir con los entregables descritos en el siguiente apartado en medio electrónico e impreso una vez validados por ambas partes.

"EL PROVEEDOR" deberá desarrollar una propuesta de los formatos y contenido de cada entregable.

"LA CEAV" podrá solicitar cualquier reporte adicional o entregable que no se cite en este apartado, así como realizar cualquier modificación que considere pertinente a los definidos en esta sección, con el objeto de respaldar la correcta entrega de los servicios o dar cumplimiento a requerimientos de solicitudes de información.

Entregables iniciales

Entregable	Descripción	Periodicidad
Acta entrega recepción y memoria técnica del servicio	"EL PROVEEDOR" deberá obtener el documento que contiene la firma de conformidad del usuario y de los responsables del servicio cuando se entregue cada uno de los sitios, dicho formato se utilizará como resguardo del equipo	Dentro de los cinco días hábiles después de la finalización de cada sitio migrado se entregarán las actas de entrega recepción.
	Memoria técnica de la instalación y diagrama de la red configurada.	Dentro de los cinco días hábiles después de la instalación y configuración de cada sitio.
Plan de Trabajo Detallado:	Presentación y entrega del Plan de Trabajo Detallado: Tareas técnicas y administrativas para la entrega, instalación y configuración, así como el cronograma de las actividades en diagrama de Gantt.	A más tardar 1 día hábil posterior a la adjudicación.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

Entregable	Descripción	Periodicidad
Procedimientos para reportar incidentes y matriz de escalación	Procedimientos para reportar incidentes y matriz de escalación	A más tardar, 5 días después de la adjudicación.
Calendario de Mantenimientos Preventivos	Calendario de Mantenimientos Preventivos	A más tardar, 30 días después de la adjudicación.
Garantías y Contratos de Soporte de los fabricantes de todos los componentes de hardware que integré a su solución.	Garantías y Contratos de Soporte de los fabricantes de todos los componentes de hardware que integré a su solución.	A más tardar, 10 días después de la finalización de instalación de los servicios.

Entregables mensuales

Entregable	Descripción	Periodicidad
Reporte mensual de niveles de servicio	<ul style="list-style-type: none">• Reporte mensual de incidentes y solicitudes de servicio en general, registradas en el sistema correspondiente de mesa de servicio.• Se deberá relacionar cada incidente con el nivel de servicio que aplique a cada caso• Este reporte deberá contemplar al menos lo siguiente:• Número de incidentes registrados en la mesa de servicio.• Estado de los incidentes y/o problemas activos.	Dentro de los cinco días hábiles del mes.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA

	<ul style="list-style-type: none">• Descripción detallada de la atención y seguimiento.• Soluciones temporales.• Soluciones permanentes.• Fecha prevista de solución.	
Reportes de Monitoreo	<p>"EL PROVEEDOR" debe de entregar un reporte de las notificaciones de todas las incidencias de equipamiento y servicios de la red, indicando que reportes ya fueron aceptados por "LA CEAV"</p> <p>"EL PROVEEDOR" debe entregar dentro de los primeros cinco días hábiles de cada mes durante la vigencia del contrato, "EL PROVEEDOR" deberá proveer reportes mensuales personalizados de acuerdo a los requerimientos de:</p> <ul style="list-style-type: none">a) Utilización de la redb) Disponibilidad de la red por segmento y localidadc) Tiempo de respuestad) Usuarios con mayor utilización de la rede) Estadísticas de tráfico y errores.f) Análisis de tendenciasg) Latencia (ms)h) Jitter (ms)i) Ancho de bandaj) Nivel de Servicio (SLA)k) Verificación de QoSl) Eventos críticos de seguridad lógica.m) Visualización en cualquier momento, en tiempo real, mediante el explorador de Internet y con una interfaz de usuario de fácil manejo para el cliente	Primero 5 días hábiles de cada mes



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA

	"EL PROVEEDOR" deberá entregar un resumen en forma impresa y/o electrónica, donde incluya el control de los cambios.	
Reporte de disponibilidad del equipamiento (Switch Core, Firewall, PBX IP, Switches Acceso, Punto de Acceso y Consolas de Monitorio)	"EL PROVEEDOR" deberá entregar un reporte mensual de los equipos y su disponibilidad.	Primero 5 días hábiles de cada mes.
Relación de inventario de equipos y licencias	"EL PROVEEDOR" deberá entregar una relación mensual de los equipos y licencias que componen la instalación.	Primero 5 días hábiles de cada mes.
Memoria Técnica	"EL PROVEEDOR" deberá entregar una memoria técnica de las Altas, Bajas y Cambios en la infraestructura en caso de presentarse.	Primero 5 días hábiles de cada mes en caso de presentarse.

Entregables Finales

Entregable	Descripción	Periodicidad
Memoria técnica y Diagrama de Red e Inventarios. (FINAL)	Memoria técnica y Diagrama de Red e Inventarios	30 días naturales previos al término de la vigencia del contrato. La entrega de esta documentación será requisito indispensable para la liberación de la fianza de cumplimiento correspondiente.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

7. Actividades en la Entrega de "EL SERVICIO"

"EL PROVEEDOR" será responsable de garantizar la continuidad del servicio objeto de esta contratación, a partir de las 00:01 horas del 20 de diciembre de 2019 en cada una de las oficinas de "LA CEAV".

"EL PROVEEDOR" deberá entregar el equipamiento solicitado en los domicilios señalados en el **Apéndice II**.

(Estos domicilios son enunciativos más no limitativos y podrán tener modificaciones de acuerdo a las necesidades de "LA CEAV").

7.1 Implementación

Durante la implementación "EL PROVEEDOR" deberá proveer un Administrador de Proyecto certificado encargado de la supervisión del plan de trabajo, el cual deberá ser aprobado por la Dirección de Tecnologías de la Información.

El plan de trabajo deberá estar detallado con fechas y horas de todas las actividades de entrega, instalación y configuración de los servicios.

7.1.1 Entrega, Instalación y Configuración

La entrega, instalación y configuración del equipamiento deberá estar completada a más tardar un día natural previo al inicio de la vigencia del servicio.

La configuración de conectividad deberá estar aprobada por la Dirección de Tecnologías de la Información.

"EL PROVEEDOR" deberá contemplar dentro de su plan de trabajo que "LA CEAV" no cuenta con bodega para resguardo de los equipos de cómputo.

"EL PROVEEDOR" deberá entregar a la Dirección de Tecnologías de la Información de "LA CEAV" las herramientas de gestión, monitoreo y administración configurada, funcionando y completada a más tardar en 15 días naturales después de la vigencia.

"EL PROVEEDOR" adjudicado se compromete a que durante la vigencia del contrato mantendrá actualizada la versión del software de dichas herramientas, sin costo adicional para "LA CEAV".

7.1.2 Migración



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA

La migración del equipamiento empieza al inicio de la vigencia del servicio y deberá estar completada más tardar en 30 días naturales después del inicio de la vigencia.

Deberán considerarse actividades y horarios que no afecten a la operación de **"LA CEAV"**, como se describe a continuación:

Migración de CORE: En fin, de semana, pudiendo iniciar actividades a partir de las 20:00 hrs. y debiendo terminar a más tardar el domingo a las 13:00 hrs. Se deberá considerar dentro de este horario también el roll back en caso de ser necesario. **"EL PROVEEDOR"** deberá cuidar el correcto etiquetado y peinado de cables de red.

Migración de switches de acceso: Podrá realizarse de lunes a domingo en horarios de 21:00 a 06:00 hrs. del día siguiente. Se deberá considerar dentro de este horario también el roll back en caso de ser necesario. **"EL PROVEEDOR"** deberá cuidar el correcto etiquetado y peinado de cables de red.

Migración de red inalámbrica: En fin, de semana, pudiendo iniciar actividades a partir del viernes a las 20:00 hrs. y debiendo terminar a más tardar el domingo a las 13:00 hrs. Se deberá considerar dentro de este horario también el roll back en caso de ser necesario.

Migración de Firewall: En fin de semana, pudiendo iniciar actividades a partir del viernes a las 20:00 hrs. y debiendo terminar a más tardar el domingo a las 13:00 hrs. Se deberá considerar dentro de este horario también el roll back en caso de ser necesario.

Seguridad: La instalación de consolas de administración y configuraciones de las funciones de seguridad y virtualización, así como herramienta de gestión y monitoreo podrá realizarse en horario laboral de **"LA CEAV"** de lunes a domingo en horarios de 21:00 a 06:00 hrs. del día siguiente bajo la supervisión e información de la Dirección de Tecnologías de la Información y sin afectar la operación de **"LA CEAV"**.

Migración PBX: La instalación del PBX y configuraciones de sus funciones, así como de servidores de los sistemas de grabación, tarificación, call center podrá realizarse en horario laboral de **"LA CEAV"** de lunes a domingo en horarios de 21:00 a 06:00 hrs. del día siguiente bajo la supervisión e información de la Dirección de Tecnologías de la Información y sin afectar la operación de **"LA CEAV"**.

Después de la migración de CORE, Switches de acceso, red inalámbrica y Firewall, **"EL PROVEEDOR"** deberá asignar al personal que realizó la migración,



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

instalación o configuración para atender incidentes que se puedan derivar de los cambios realizados hasta tener el visto bueno de la Dirección de Tecnologías de la Información de "LA CEAV".

7.2 Transferencia de Conocimiento

Al término de la instalación, "EL PROVEEDOR" deberá proporcionar las configuraciones y scripts implementados y deberá contestar todas las dudas que "LA CEAV" presente al respecto.

Después de la atención de algún incidente o atención a un reporte por petición de soporte "EL PROVEEDOR" deberá proporcionar las configuraciones y scripts implementados y deberá contestar todas las dudas que "LA CEAV" presente al respecto.

Como parte de la transferencia del conocimiento, "EL PROVEEDOR" adjudicado deberá proporcionar sin costo adicional para "LA CEAV" un curso y certificación de operación básica para la Solución Voz, Datos y Seguridad para dos personas, que incluya configuración de VLANs, configuración de puertos, tablas de ARP, revisión de logs, PoE, detección de loops. Este curso será impartido en las instalaciones de "LA CEAV" por parte de personal del proveedor adjudicado que cuente con certificación del fabricante de la tecnología utilizada.

8. Metodología

El PMBOK (Project Management Body of Knowledge) es un documento que reúne el conocimiento relacionado con la Dirección de Proyectos, por lo cual "EL PROVEEDOR" deberá contar con esta metodología para la entrega de "EL SERVICIO".

"EL PROVEEDOR" deberá apegarse a lo establecido en el Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTIC-SI), para el diseño, instalación, administración y operación de la solución.

La mesa de ayuda del proveedor deberá estar alineada a ITIL (Information Technology Infrastructure Library).

9. Administrador del Contrato

El Ing. Rogelio Mesta Estrada, Titular de la Dirección de Tecnologías de la Información, o quien lo sustituya o supla, serán responsables de administrar, validar y supervisar el cumplimiento de "EL SERVICIO".



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

10. Lugar de Entrega de "EL SERVICIO"

La entrega de "EL SERVICIO" se realizará en los domicilios señalados en el **Apéndice II**.

11. Informe a Entregar.

Referirse al numeral 6 del presente **Anexo I**.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

APÉNDICE I

Cantidad estimada de equipos a suministrar.

Catálogo de Servicios:

No.	Descripción	Cantidad Mínima	Cantidad Máxima	Unidad Medida	de
1	Switch Core Sitio Central	1	1	Pieza	
2	Switches de Acceso Tipo A de 48 pts	5	8	Pieza	
3	Switches de Acceso Tipo B de 24 pts	42	45	Pieza	
4	Controlador Wireless	2	2	Pieza	
5	Puntos de Acceso	44	47	Pieza	
6	UTM Tipo A Central	2	2	Pieza	
7	UTM Tipo B Remoto	32	35	Pieza	
9	Cliente UTM para PC para preservar políticas corporativas	0	1	Cliente	
9	Sistema de Administrador de llamadas de telefonía IP	1	1	Pieza	
10	Sistema de Telefonía IP y Gateway Sitio Central	1	1	Pieza	
11	Mensajería Unificada	0	1	Pieza	
12	Gateway Sitio Remoto	22	25	Pieza	
13	Gateway Sitio Remoto Tipo 2 (Sin Redundancia)	9	12	Pieza	
14	Aparato Telefónico IP Básica	402	442	Pieza	
15	Aparato Telefónico IP Semi Ejecutiva	79	82	Pieza	
16	Terminal Audio Conferencia	2	5	Pieza	
17	Aparato Telefónico IP Secretarial	29	32	Pieza	
18	Aparato Telefonico IP Call Center	4	7	Pieza	
19	Terminal IP Basada en Software	2	35	Pieza	
20	Consola Operadora	1	1	Pieza	
21	Sistema Contact Center	4	5	Usuario	
22	Sistema Grabación	1	1	Pieza	
23	Sistema Tarificación	1	1	Pieza	
24	UPS 1.5 KVA	33	36	Pieza	
25	UPS 3 KVA	3	6	Pieza	
26	UPS 5 KVA	1	4	Pieza	
27	Rack 40U Central	1	4	Pieza	
28	Rack 20U Remoto	32	35	Pieza	



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

29	Sistema de Monitoreo de Desempeño de los Componentes de Red	140	160	Componente
30	Cambio de domicilio	0	5	Sitio
31	Servicio de Cableado Estructurado	0	100	Nodo

El Catálogo de Servicio deberá considerar el listado de Hardware y Software necesario para su instalación y configuración.

En caso de requerir un servicio no incluido en el Catálogo de Servicio, "LA CEAV" solicitará una cotización a "EL PROVEEDOR" para su evaluación.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

APÉNDICE II

La entrega de "EL SERVICIO" se realizará en los domicilios señalados a continuación:

No.	Domicilio	Ubicación
1	Oficina Central	Ángel Urraza 1137, Del Valle, Benito Juárez, Ciudad de México. C.P. 03100
2	CAI CDMX	Ángel Urraza 1013, Del Valle, Benito Juárez, Ciudad de México. C.P. 03100
3	CAI Baja California	Calle Monterrey número 3130, Sección B, colonia Mineral de Santa Fe, C.P. 22415, Tijuana, Baja California.
4	CAI Chiapas	Palacio Federal, calle Segunda Oriente Norte número 227, primer piso, colonia Centro, C.P. 29000, Tuxtla Gutiérrez, Chiapas.
5	CAI Chiapas-Tapachula	Segunda Avenida Norte número 1, entre Avenida Central y Primera Poniente, Colonia Centro, C.P. 30700, Tapachula, Chiapas.
6	CAI Chihuahua	Juan de la Barrera No. 661, Esq. Av. Insurgentes, Fraccionamiento La Joya, C.P. 32330, Ciudad Juárez, Chihuahua.
7	CAI Coahuila	Palacio Federal, Av. Juárez esquina Ramón Corona, segundo piso, despacho 304, colonia Centro, C.P. 27000, Torreón, Coahuila.
8	CAI Guanajuato	Carretera Guanajuato-Juventino Rosas Km 7.5, colonia Arroyo Verde, C.P. 36250, Guanajuato, Guanajuato.
9	CAI Guerrero	Calle Almirante Fernando de Magallanes esquina con Parque Sur, Lote 1, Manzana 28, Fraccionamiento Costa Azul, C.P. 39850, Acapulco, Guerrero.
10	CAI Jalisco	Avenida Unión número 199, esquina Avenida La Paz, colonia americana, C.P. 44100, Guadalajara, Jalisco.
11	CAI Michoacán	Avenida Acueducto número 1464, colonia Chapultepec Norte, Sector Nueva España, C.P. 58260, Morelia, Michoacán.



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA

- | | | |
|----|-------------------------|--|
| 12 | CAI Morelos | Río Amacuzac número 24, esquina con Calzada de Los Estrada, colonia Vista Hermosa, C.P. 62290, Cuernavaca, Morelos. |
| 13 | CAI Nayarit | Calle Encino número 11, esquina Avenida Jacarandas, colonia San Juan, C.P. 63130, Tepic, Nayarit. |
| 14 | CAI Nuevo León | Calle Porfirio Díaz Sur número 1425, colonia Pío X, C.P. 64710, Monterrey, Nuevo León. |
| 15 | CAI Sinaloa | Avenida General Álvaro Obregón número 1298 Sur, colonia Guadalupe, C.P. 80220, Culiacán, Sinaloa. |
| 16 | CAI Veracruz | Avenida Gómez Farías número 2125, colonia Ricardo Flores Magón, C.P. 91900, Veracruz, Veracruz. |
| 17 | CAI Yucatán | Calle 33 B número 185, esquina calle 8, colonia García Ginerés, C.P. 97070, Mérida, Yucatán. |
| 18 | CAI Durango | Calle Camino del Amanecer número 470, Fraccionamiento Los Remedios, C.P. 34100, Durango, Durango. |
| 19 | CAI Aguascalientes | Calle Coquimbo número 104, Fraccionamiento La Fuente, C.P. 20239, Aguascalientes, Aguascalientes. |
| 20 | CAI Baja California Sur | Calle Dionisia Villarino número 2130 tercer piso, entre Ignacio Allende y Benito Juárez, Fraccionamiento Perla, colonia Centro, C.P. 23000, La Paz, Baja California Sur (Edificio BANOBRAS). |
| 21 | CAI Campeche | Avenida 16 de septiembre S/N, colonia Centro, C.P. 24000, San Francisco de Campeche, Campeche. |
| 22 | CAI Colima | Calle Francisco I. Madero número 243, colonia Centro, C.P. 28000, Colima, Colima. |
| 23 | CAI Estado de México | Calle Ezequiel Ordóñez número 108, Barrio de la Merced, C.P. 50080, Toluca de Lerdo, Estado de México. |
| 24 | CAI Hidalgo | Avenida Gabriel Hernández número 106, colonia Periodistas, C.P. 42060, Pachuca de Soto, Hidalgo. |
| 25 | CAI Oaxaca | Calle Amapolas número 1100, segundo piso, colonia Reforma, C.P. 68050, Oaxaca de Juárez, Oaxaca. |



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

- | | | |
|----|---------------------|--|
| 26 | CAI Puebla | Palacio Federal, calle 5 Oriente número 1, primer piso, esquina 16 de septiembre, colonia Centro, C.P. 72000, Puebla, Puebla. |
| 27 | CAI Querétaro | Calle Wenceslao de la Barquera número 13 esquina con Leopoldo Aguilar, colonia Villas del Sur, C.P. 76040, Querétaro, Querétaro. |
| 28 | CAI Quintana Roo | Calle Gladiolas Retorno 7 número 19, supermanzana 22, Manzana 20, C.P. 77500, Benito Juárez, Cancún, Quintana Roo. |
| 29 | CAI San Luis Potosí | Avenida Chapultepec número 1256, Interior Local 5, colonia Privadas del Pedregal, C.P. 78295, San Luis Potosí, San Luis Potosí. |
| 30 | CAI Sonora | Palacio Federal, calle Rosales S/N, entre Aquiles Serdán y Plutarco Elías Calles, colonia Centro, C.P. 83000, Hermosillo, Sonora. |
| 31 | CAI Tabasco | Privada del Caminero número 17, colonia Primero de Mayo, C.P. 86190, Villahermosa, Tabasco. |
| 32 | CAI Tamaulipas | Palacio Federal cuarto piso, calle Juan B. Tijerina S/N entre José María Morelos y Mariano Matamoros, colonia Centro, C.P. 87000, Ciudad Victoria, Tamaulipas. |
| 33 | CAI Tlaxcala | Calle Porfirio Díaz número 10, colonia Centro, C.P. 90000, Tlaxcala, Tlaxcala. |
| 34 | CAI Zacatecas | Avenida Universidad número 246, colonia La Loma, C.P. 98068, Zacatecas, Zacatecas. |

Nota: Estos sitios son enunciativos más no limitativos y podrán tener modificaciones de acuerdo a las necesidades de "LA CEAV".



CEAV
COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

Leído por "LAS PARTES" y enteradas de su contenido y alcance legal, se firma el presente **Anexo I** del Contrato **CEAV-C-56-2019**, libre de vicios en el consentimiento, tales como error, dolo, mala fe o violencia, en tres tantos, en la Ciudad de México, el día 29 de noviembre de 2019.

POR "LA CEAV"

DIRECCIÓN GENERAL DE
ADMINISTRACIÓN Y FINANZAS

POR "EL PROVEEDOR"

C. CRISTÓBAL ERNESTO GARCÍA VEGA
APODERADO LEGAL
ORBEN COMUNICACIONES, S.A.P.I. DE C.V.

En suplencia por ausencia de la persona Titular de la Dirección General de Administración y Finanzas con fundamento en los artículos 5, fracción XI inciso c; 23 bis párrafo segundo y 34 fracción XVIII del Estatuto Orgánico de la Comisión Ejecutiva de Atención a Víctimas, última reforma publicada en el Diario Oficial de la Federación el 20 de diciembre de 2018, suscribe el presente Contrato el Director de Recursos Materiales y Servicios Generales, el C.P. Salvador Osogobio Villegas.

POR "EL ADMINISTRADOR DEL
CONTRATO"

ING. ROGELIO MESTA ESTRADA
DIRECTOR DE TECNOLOGÍAS DE LA
INFORMACIÓN

Las firmas que anteceden forman parte del **Anexo I** del Contrato número **CEAV-C-56-2019**, celebrado entre la **COMISIÓN EJECUTIVA DE ATENCIÓN A VÍCTIMAS** y **ORBEN COMUNICACIONES, S.A.P.I. DE C.V.**



CEAV

COMISIÓN EJECUTIVA
DE ATENCIÓN A VÍCTIMAS

CEAV-C-56-2019

"SERVICIO INTEGRAL DE RED LOCAL, RED AMPLIA, SEGURIDAD PERIMETRAL Y TELEFONÍA"

Anexo II

PROPUESTA ECONÓMICA DE "EL PROVEEDOR"



Anexo Propuesta Económica

PARTIDA	DESCRIPCIÓN	CANTIDAD	UNIDAD DE MEDIDA	PRECIO UNITARIO	SUBTOTAL MENSUAL
UNICA	Switch Core-Silo Central	1	Pieza	\$ 15,185.15	\$ 15,185.15
	Switches de Acceso Tipo A de 48 puo	6	Pieza	\$ 1,794.17	\$ 10,765.02
	Switches de Acceso Tipo B de 24 puo	43	Pieza	\$ 682.90	\$ 29,364.70
	Controlador Wireless	2	Pieza	\$ 7,430.20	\$ 14,860.40
	Puntos de Acceso	48	Pieza	\$ 298.22	\$ 12,419.90
	UTM Tipo A Central	2	Pieza	\$ 21,035.93	\$ 42,071.86
	UTM Tipo B Ramal	23	Pieza	\$ 1,904.99	\$ 44,804.77
	UTM Tipo C Ramal	10	Pieza	\$ 9,967.88	\$ 99,678.80
	Disco UTM para PC para preservar políticas corporativas	0	Cliente	\$ 46.88	\$ -
	Sistema de Administrador de Usuarios de Telefonía IP	1	Pieza	\$ 15,072.47	\$ 15,072.47
	Sistema de Telefonía IP y Gateway Silo Central	1	Pieza	\$ 7,019.83	\$ 7,019.83
	Mensajería Unificada	0	Pieza	\$ 8,268.85	\$ -
	Gateway Silo Ramal	23	Pieza	\$ 2,400.39	\$ 55,209.07
	Gateway Silo Ramal Tipo 2 (Sin Redundancia)	18	Pieza	\$ 2,599.80	\$ 25,998.80
	Aparato Telefónico IP Básica	402	Pieza	\$ 65.32	\$ 26,258.84
	Aparato Telefónico IP Semi Ejecutiva	80	Pieza	\$ 65.32	\$ 5,225.80
	Terminal Audio Conferencia	3	Pieza	\$ 345.19	\$ 1,036.57
	Aparato Telefónico IP Secretarial	20	Pieza	\$ 150.53	\$ 3,010.60
	Aparato Telefónico IP Call Center	5	Pieza	\$ 78.23	\$ 391.15
	Terminal IP Basada en Software	2	Pieza	\$ 75.80	\$ 151.60
	Consola Operadora	1	Pieza	\$ 2,804.12	\$ 2,804.12
	Sistema Contact Center	5	Usuario	\$ 385.42	\$ 1,927.10
	Sistema Grabación	1	Pieza	\$ 2,710.14	\$ 2,710.14
	Sistema Tarifación	1	Pieza	\$ 4,647.65	\$ 4,647.65
	UPS 1.5 KVA	34	Pieza	\$ 1,217.24	\$ 41,386.16
	UPS 3 KW	4	Pieza	\$ 500.96	\$ 2,003.84
	UPS 5 KVA	2	Pieza	\$ 3,057.26	\$ 6,114.52
	Rack 40U Central	2	Pieza	\$ 1,773.06	\$ 3,546.12
Rack 20U Ramal	33	Pieza	\$ 451.85	\$ 14,911.05	



Sistema de Atención de Desempeño de los Componentes de Red	150	Componente	\$ 73.26	\$ 10,989.00
Cambio de Domicilio			\$ 12,000.00	\$ -
Sistema de Cableado estructurado			\$ 7,000.00	\$ -
TOTAL			\$	\$ 905,442.85
IVA			\$	\$ 80,876.00
TOTAL			\$	\$ 986,318.71

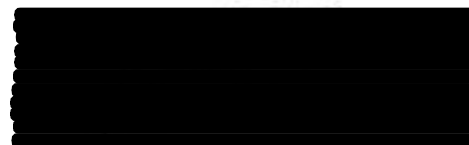
La propuesta mensual de Orben Comunicaciones SAPI de CV para el Servicio Integral de Red Local, Red Amplia, Seguridad Perimetral y Telefonía para la Comisión Ejecutiva de Atención a Víctimas asciende a: **Quinientos ochenta y seis mil trescientos trece pesos 71/100 Moneda Nacional**

Nota importante: Los precios de Orben Comunicaciones SAPI de CV son con equipos usados / adquiridos nuevos y originales de fabrica para el contrato CEAV / Contrato **CEAV-C-51-2015**

Condiciones Comerciales:

- Los precios están en Moneda Nacional
- Los precios incluyen IVA
- Plazo de contratación: 20 de diciembre 2019 al 30 de abril 2020
- Lugar de entrega: Instalaciones de CEAV
- Tiempo de entrega de servicios: **Inmediato**
- Condiciones de Pago: Pagos Mensuales
- Vigencia de la Propuesta: 60 días naturales

Atentamente



Patricia Olivares Vazquez
Ejecutiva de Ventas
Orben Comunicaciones S.A.P.I. de C.V.