ITP-019/2024

CONTRATO CERRADO PARA LA PRESTACIÓN DEL SERVICIO DE ARRENDAMIENTO DE EQUIPO PARA TELEFONÍA IP, CON CARÁCTER NACIONAL QUE CELEBRAN POR UNA PARTE, EL EJECUTIVO FEDERAL POR CONDUCTO DEL INSTITUTO NACIONAL PARA LA EDUCACIÓN DE LOS ADULTOS, EN LO SUCESIVO "EL INEA", REPRESENTADO POR LA C. MARÍA ISABEL MONTOYA OBREGÓN, EN SU CARÁCTER DE APODERADA LEGAL Y TITULAR DE LA UNIDAD DE ADMINISTRACIÓN Y FINANZAS, ASISTIDA EN ESTE ACTO POR LA C. MARÍA DOLORES DURÁN MÁRQUEZ, SUBDIRECTORA DE RECURSOS TECNOLÓGICOS, QUIEN FUNGIRÁ COMO PERSONA ADMINISTRADORA DEL CONTRATO, ASÍ COMO EL C. ROBERTO RAMÍREZ GUZMÁN, JEFE DE DEPARTAMENTO DE SOPORTE TÉCNICO, CENTRO DE DATOS Y COMUNICACIÓN, QUIEN FUNGIRÁ COMO PERSONA SUPERVISORA DEL CONTRATO Y POR LA OTRA, REISCOM, S.A. DE C.V. EN LO SUCESIVO "EL PROVEEDOR", REPRESENTADA POR EL C. FRANCISCO JAVIER MURILLO PANTOJA, EN SU CARÁCTER DE APODERADO LEGAL, A QUIENES DE MANERA CONJUNTA SE LES DENOMINARÁ "LAS PARTES", AL TENOR DE LAS DECLARACIONES Y CLÁUSULAS SIGUIENTES:

I. "EL INEA" declara que:

I.1 Es un Organismo Descentralizado de la Administración Pública Federal, agrupado en el sector coordinado por la Secretaría de Educación Pública y Subsecretaría de Educación Básica con personalidad jurídica y patrimonio propio, creado por Decreto Presidencial el 28 de agosto de 1981, publicado en el Diario Oficial de la Federación (DOF) el 31 de ese mismo mes y año, reformado por diverso de fecha 17 de agosto de 2012, publicado en el DOF el 23 de agosto de 2012.

I.2 Conforme a la escritura pública número 79,644 de fecha 20 de febrero de 2024, pasada ante la fe de la Lic. Liliana Gutiérrez Robles, titular de la notaría pública número 44 de la Ciudad de México, la C. María Isabel Montoya Obregón con R.F.C. MOOI570119MR9, Apoderada legal y Titular de Unidad de Administración y Finanzas de **"EL INEA"**, es la persona servidora pública que cuenta con facultades legales para celebrar el presente contrato, quien podrá ser sustituida en cualquier momento en su cargo o funciones, sin que por ello, sea necesario celebrar un convenio modificatorio.

I.3 De conformidad con el *Manual General de* Organización del INEA 2020, suscribe el presente instrumento jurídico el C. María Dolores Durán Márquez, en su carácter de Subdirectora de Recursos Tecnológicos, con R.F.C. DUMD6808112R5, persona facultada para administrar, dar seguimiento y verificar el cumplimiento de las obligaciones que deriven del objeto del presente contrato, quien podrá ser sustituido en cualquier momento, bastando para tales efectos un comunicado por escrito y firmado por el servidor público facultado para ello, informando a **"EL PROVEEDOR"** para los efectos del presente contrato.

I.4 De conformidad con el Manual General de Organización del INEA 2020, suscribe el presente instrumento jurídico el C. Roberto Ramírez Guzmán, Jefe de Departamento de

Francisco Márquez 160, Col . Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea

Soporte Técnico, Centro de Datos y Comunicación, con RFC RAGR740522162, persona facultada para supervisar los bienes y/o servicios conforme a los términos y condiciones establecidos en el Contrato y su **"ANEXO ÚNICO"**, (el cual se conforma por Anexo 1.- Anexo Técnico y sus Apéndices, propuesta técnica y económica), que forman parte integrante del mismo.

I.5 La contratación del presente instrumento se realizó mediante el procedimiento de Invitación a cuando menos tres personas y medio electrónico de carácter nacional número IA-11-MDA-011MDA001-N-59-2024, **SERVICIO DE ARRENDAMIENTO DE EQUIPO PARA TELEFONÍA IP**, al amparo de lo establecido en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos; y los artículos 26 fracción II, 26 Bis fracción II, 28 fracción I, 40 párrafo tercero, 42 párrafo primero y tercero, 43 y 45 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público en lo sucesivo la **"LAASSP"**; y 81 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público en lo sucesivo el **"RLAASSP"**

I.6 "EL INEA" cuenta con suficiencia presupuestaria otorgada mediante cédula SRT/018/2024 de fecha 12 de marzo de 2024, emitida por la Subdirección de Presupuesto y Recursos Financieros, aplicada en la partida 32301 "Arrendamiento de Equipos y Bienes Informáticos" emitida por la Subdirección de Presupuesto y Recursos Financieros.

I.7 Para efectos fiscales las Autoridades Hacendarias le han asignado el Registro Federal de Contribuyentes INE810901CP4.

I.8 Para los efectos del presente contrato, señala como su domicilio el ubicado en calle Francisco Márquez número 160, colonia Condesa, código postal 06140, demarcación territorial Cuauhtémoc, Ciudad de México.

II. "EL PROVEEDOR" declara que:

II.1 Es una persona moral legalmente constituida mediante la escritura número 239,930 de fecha 10 de diciembre de 2007, otorgada ante la fe del Lic. Fausto Rico Álvarez, titular de la notaría 6, del Distrito Federal hoy Ciudad de México, misma que ha sufrido modificaciones, denominada REISCOM DE MÉXICO, S.A. DE C.V., cuyo objeto social es, la compra, venta, distribución y mantenimiento de equipos y sistemas de telecomunicaciones, datos, cómputo, video y los distintos periféricos, programas y sistemas operativos necesarios para la operación de los mismos; diseño, ejecución, reparación y mantenimiento de cableados telefónicos convencionales, cableados estructurados y cableados eléctricos relacionados con sistema de telecomunicación.

II.2 Francisco Javier Murillo Pantoja en su carácter de Apoderado Legal, cuenta con facultades suficientes para suscribir el presente contrato y obligar a su representada, como lo acredita con la escritura pública número 239,930 de fecha 10 de diciembre de 2007, otorgada ante la fe de la Lic. Fausto Rico Álvarez, titular de la notaría 6, del Distrito Federal hoy Ciudad de México, mismas que bajo protesta de decir verdad manifiesta no le han sido limitadas ni revocadas en forma alguna.

Francisco Márquez 160, Col . Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea

II.3 Reúne las condiciones técnicas, jurídicas y económicas, y cuenta con la organización y elementos necesarios para su cumplimiento.

II.4 Cuenta con su Registro Federal de Contribuyentes REI0409133L4

II.5 Bajo protesta de decir verdad, está al corriente en los pagos de las obligaciones fiscales, en específico las previstas en el artículo 32-D del Código Fiscal Federal vigente, así como de sus obligaciones fiscales en materia de seguridad social, ante el Instituto Nacional de la Vivienda para los Trabajadores (INFONAVIT) y en el Instituto Mexicano del Seguro Social (IMSS); lo que acredita con la Opinión de Cumplimiento de Obligaciones Fiscales y en materia de Seguridad Social en sentido positivo, emitidas por el SAT e IMSS, respectivamente, así como las Constancias de Situación Fiscal en materia de Aportaciones Patronales y Entero de Descuentos, sin adeudo, emitida por el INFONAVIT, las cuales se encuentran vigentes y obran en el expediente respectivo.

II.6 Tiene establecido su domicilio en calle atlapulco número 6-A, colonia Vergel del Sur, demarcación territorial Tlalpan, código postal 14340, Entidad Federativa Ciudad de México, mismo que señala para los fines y efectos legales del presente contrato.

III. "LAS PARTES" declaran que:

III.1 Es su voluntad celebrar el presente contrato y sujetarse a sus términos y condiciones, por lo que de común acuerdo se obligan de conformidad con las siguientes:

CLÁUSULAS

PRIMERA. OBJETO DEL CONTRATO.
"EL PROVEEDOR" acepta y se obliga a proporcionar a **"EL INEA"** la prestación del **SERVICIO DE ARRENDAMIENTO DE EQUIPO PARA TELEFONÍA IP,** en los términos y condiciones establecidos en este contrato y su **"ANEXO ÚNICO"** (el cual se conforma por la propuesta técnica y económica), que forman parte integrante del mismo.

SEGUNDA. MONTO DEL CONTRATO.
"EL INEA" pagará a **"EL PROVEEDOR"** como contraprestación por los servicios objeto de este contrato, la cantidad de **$1'556,940.00 (Un millón quinientos cincuenta y seis mil novecientos cuarenta pesos 00/100 M.N.)** más impuestos que ascienden a **$249,110.40 (Doscientos cuarenta y nueve mil ciento diez pesos 40/100 M.N.),** dando un monto total de **$1'806,050.40 (Un millón ochocientos seis mil cincuenta pesos 40/100 M.N.)**

No.	PRODUCTO	CANTIDAD	COSTO UNITARIO MENSUAL	COSTO TOTAL JUNIO A DICIEMBRE 2024
1	TERMINAL IP BASICA	142	$935.00	$929,390.00
2	TERMINAL IP EJECUTIVA	40	$1,910.00	$534,800.00

Francisco Márquez 160, Col . Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea

3	SERVICIO DE TARIFACIÓN TELEFÓNICA PARA 649 EXTENSIONES	1	$13,250.00	$92,750.00
		SUBTOTAL	$495.30	$1’556,940.00
		IVA	$79.25	$249,110.40
		TOTAL	$574.55	$1’806,050.40

TERCERA. ANTICIPO.
Para el presente contrato **“EL INEA”** no otorgará anticipo a **“EL PROVEEDOR”**.

CUARTA. FORMA Y LUGAR DE PAGO.
“EL INEA” efectuará el pago a través de transferencia electrónica en pesos de los Estados Unidos Mexicanos, en moneda nacional por servicios devengados, en función del importe generado por los servicios prestados a entera satisfacción, durante ese lapso, los cuales deberán estar debidamente validados y aprobados por el supervisor del Instrumento Jurídico de las Oficinas Centrales de **“El INEA”** y de acuerdo con lo establecido en el **“ANEXO ÚNICO”** que forma parte integrante de este contrato.

Con fundamento en el artículo 51 de la “LAASSP” el pago no podrá exceder de 20 (veinte) días naturales contados a partir de la entrega de la factura respectiva, previa entrega de los bienes y/o servicios en los términos del instrumento jurídico y a entera satisfacción del Administrador (a) del contrato, según lo establecido en su **“ANEXO ÚNICO”**

Para que **“EL INEA”,** esté en condiciones de iniciar las gestiones de pago, “**EL PROVEEDOR”** de conformidad a lo establecido en el **“ANEXO ÚNICO”** y a los artículos **29** y **29-A** del **Código Fiscal de la Federación** y los correlativos de su Reglamento, está obligado a enviar al Supervisor (a) del contrato el **Comprobante Fiscal Digital por Internet (CFDI)**, así como sus archivos electrónicos **.XML y .PDF**

“EL PROVEEDOR” para la elaboración del **CFDI** deberán considerar lo siguiente:

- **Emitido a nombre de**: Instituto Nacional para la Educación de los Adultos.
- **RFC:** INE810901CP4.
- **Domicilio**: Calle Francisco Márquez número 160, colonia Condesa, código postal 06140, demarcación territorial Cuauhtémoc, Ciudad de México.
- **Régimen Fiscal**: 603 personas morales con fines no lucrativos.
- **Uso del CFDI**: Gastos en general.
- **Rubro concepto/descripción**: indicar si es pago único, o el número de pago que corresponda, ejemplo: primer o segundo pago del contrato, número de contrato o convenio, mes de pago en caso de que aplique y descripción breve del servicio realizado o producto adquirido.
- **Forma de pago**: Transferencia electrónica.
- **Método de pago**: Pago en parcialidades o diferido (PPD)
- **Todos los CFDI deberán ser emitidos en la versión 4.0.**

Francisco Márquez 160, Col . Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea

"EL PROVEEDOR", antes de emitir el **CFDI** para su pago, deberá enviar al Supervisor (a) del contrato, por medio de correo electrónico, un proyecto del mismo. Lo anterior, con la finalidad de que el Supervisor (a) valide o realice las observaciones correspondientes y posteriormente **"EL PROVEEDOR"** emita y envíe la versión final del **CFDI**.

"EL PROVEEDOR", deberá enviar vía correo electrónico al Supervisor (a), dentro de los primeros 3 (tres) días naturales del mes calendario o del mes que corresponda, la versión final timbrada del **CFDI (dentro de este plazo queda comprendido el párrafo que antecede)**; éste último contará con 3 (tres) días hábiles a partir de la recepción del **CFDI**, para devolverla con las observaciones pertinentes o, en su caso, iniciar la gestión de pago con la aceptación de la versión final timbrada.

Una vez aceptada la versión final timbrada del **CFDI**, el Administrador (a) del contrato la enviará junto con sus archivos electrónicos **.XML y .PDF**, por correo electrónico al Departamento de Control Presupuestal **(DCP)** de **"EL INEA"** (ifrias@inea.gob.mx y dpc_control@inea.gob.mx).
El Administrador (a) del contrato, independientemente de lo señalado en el párrafo previo, también deberá entregar a la Subdirección de Presupuesto y Recursos Financieros **(SPRF),** dentro de los primeros 12 (doce) días naturales del mes de que se trate, contados a partir de la recepción de la factura timbrada y soporte documental respectivo, el oficio o nota debidamente firmado por el mismo, a través del cual se entrega el soporte documental del pago correspondiente y que contendrá lo siguiente:

- 3 (tres) tantos de la *Solicitud de Recursos para Pedidos y Contratos*, firmada en original por el Administrador (a) del contrato correspondiente y el Titular del área requirente.
- Impresión de **CFDI, XML** y verificación del SAT.
- Copia del oficio de liberación de pago firmado por el Administrador (a) del contrato.
- Copia del oficio de supervisión del servicio dirigido al Administrador (a) del contrato y que será firmado por el Supervisor (a) del mismo.
- Copia de la suficiencia presupuestal
- Para el trámite del **primer pago** deberá también adjuntar a la solicitud copia del contrato o convenio.
- En caso de **último pago** deberá también adjuntar copias de la Constancia de cumplimiento y del finiquito conforme lo consigne el contrato.

Si por algún motivo se cancela el **CFDI** durante el proceso de pago, será responsabilidad de **"EL PROVEEDOR"** notificar por escrito al Administrador (a) del contrato, quien a su vez informará por escrito a la **SPRF.**

Los pagos se efectuarán a través de Cuentas por Liquidar Certificadas (CLC), apoyados en los mecanismos de banca electrónica del Sistema Integral de Administración Financiera Federal **(SIAFF)** de la Tesorería de la Federación mediante enlace con el **Sistema de Contabilidad y Presupuesto (SICOP)** por instrucción de la **Unidad de Administración y Finanzas** mediante **transferencia electrónica de**

Francisco Márquez 160, Col . Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea

recursos a la cuenta bancaria señalada por **"EL PROVEEDOR"** previamente registrada, por el importe del servicio proporcionado.

Para dar cumplimiento a lo anterior, será indispensable que **"EL PROVEEDOR"** entregue al Departamento de Tesorería **(DT)**, dentro de los 3 (tres) días hábiles posteriores al fallo, la documentación de forma física y electrónica que se cita abajo, con la finalidad de dar de alta en los Sistemas Federales de pago, Sistema de Contabilidad y Presupuesto **SICOP** y **SIAFF** de la Tesorería de la Federación:

a) Acta constitutiva inscrita en el Registro Público de la Propiedad y del Comercio, así como sus respectivas modificaciones.

b) Copia del instrumento notarial donde consten las facultades de representante y/o apoderado legal.

c) Identificación oficial vigente (credencial de elector o cartilla del servicio militar nacional o cédula profesional o pasaporte) de la persona que se ostente como representante y/o apoderado legal.

d) Copia de la Constancia de Situación Fiscal y Registro Federal de Contribuyentes **(RFC)** expedido por la Secretaría de Hacienda y Crédito Público **(SHCP)** no mayor a 3 (tres) meses.

e) Formato del Catálogo de Beneficiarios debidamente requisitado, con sello de la empresa y firma autógrafa del representante y/o apoderado legal, que podrá descargar para su llenado en la siguiente liga:

   https://www.sep.gob.mx/es/sep1/Formatos_Vigentes o solicitarlo al **DT** a las siguientes direcciones de correo electrónico: juangc@inea.gob.mx; dt_pagos@inea.gob.mx.

f) Constancia del domicilio fiscal no mayor a 3 (tres) meses.

g) Para el caso de personas físicas, copia de la Clave Única de Registro de Población **(CURP)**.

h) Constancia de la institución financiera sobre la existencia de la cuenta de cheques abierta a nombre del beneficiario, que incluya el número de cuenta con once posiciones, así como la clave bancaria estandarizada (CLABE) con dieciocho posiciones, que permita realizar transferencias electrónicas de fondos a través de los sistemas federales de pagos, esta debe incluir la sucursal de apertura de la cuenta bancaria.

"EL INEA" pagará a **"EL PROVEEDOR"**, conforme a las condiciones que se consignan en el contrato y su **"ANEXO ÚNICO".**

Francisco Márquez 160, Col . Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea

El Administrador (a) y **"EL PROVEEDOR"**, serán los únicos responsables de realizar el cálculo en caso de pagos en exceso, **"EL PROVEEDOR"** deberá reintegrar dichas cantidades, más las cargas financieras correspondientes, conforme a una 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 de pago hasta la fecha en que se pongan efectivamente las cantidades a disposición de **"EL INEA"**. Para el efecto anterior, **"EL PROVEEDOR"** autoriza en este acto a **"EL INEA"** a deducir dichas cantidades de cualquier crédito pendiente de pago.

- **"EL PROVEEDOR" mediante oficio, firmado por el representante y/o apoderado legal, lo entregará al DT, en el que solicitará una clave RAP para efectuar el deposito referenciado a la cuenta bancaria Institucional por la devolución del recurso pagado en exceso.**

- **"EL PROVEEDOR" deberá remitir el comprobante de pago al DT por el monto de la devolución del recurso y en su caso pagar las cargas financieras que pudieran generar en caso de no devolver el recurso en el ejercicio fiscal correspondiente.**

El Administrador (a) y/o Supervisor (a) del contrato serán responsables de dar seguimiento al pago de **"EL PROVEEDOR"**, de cualquier accesorio que se genere por incumplimiento al contrato y hasta su liberación.

Si el **"EL PROVEEDOR"** estuviere inconforme con la liquidación del pago, tendrá un plazo de 10 (diez) días naturales, a partir de la fecha en que se haya formulado la liquidación del pago, para hacer por escrito la reclamación dirigida a la **Unidad de Administración y Finanzas**. Si transcurrido este plazo, **"EL PROVEEDOR"** no la efectúa, se considerará que la liquidación del pago, quedará definitivamente aceptada por él y sin derecho a ulterior reclamación.

De acuerdo a la obligación de emitir facturas **"CFDI con Complemento para la Recepción de Pagos"** en cumplimiento a la regla **2.7.1.32** de la Resolución Miscelánea Fiscal para el ejercicio 2024.

Los escenarios para emitir el **CFDI** con Complemento para la Recepción de Pagos (Recibo Electrónico de Pagos), son los siguientes:

1. Al emitir el **CFDI** y hacer el pago en ese momento, **no hay obligación de emitir el complemento de pago,** el **CFDI** debe contener los siguientes datos en la forma de pago: 03 Transferencia electrónica de fondos, Método de pago: PUE (Pago en Una sola Exhibición).

2. Al emitir el **CFDI** y **el pago se hace posteriormente**, es decir al hacer un **pago diferido (PPD)** del total de la factura, **se deberá emitir el complemento de pago**. El **CFDI** del complemento deberá tener los siguientes datos: Cantidad: 1; Unidad: ACT;

Francisco Márquez 160, Col . Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea

Descripción: Pago; Clave Prod. Serv. 84111506 Servicios de facturación. Precio unitario 0 (cero); Importe 0 (cero).

3. Al emitir el **CFDI** y el pago se hace **en parcialidades (PPD) se deberá hacer el complemento por el pago de cada parcialidad**. El **CFDI** del complemento deberá tener los siguientes datos: Cantidad: 1; Unidad: ACT; Descripción: Pago; Clave Prod. Serv. 84111506 Servicios de facturación. Precio unitario 0 (cero); Importe 0 (cero).

El Supervisor (a) del contrato solicitará a **"EL PROVEEDOR"** el **"CFDI con Complemento para la Recepción de Pagos",** quien la deberá emitir en el periodo de 10 (diez) días naturales del mes inmediato siguiente en que se recibieron los pagos.

"EL PROVEEDOR" enviará los **"CFDI con Complemento para la Recepción de Pagos"** al correo electrónico del Administrador (a) del Contrato y al correo del Departamento de Contabilidad **(DC)** de **"EL INEA"** ldelrio@inea.gob.mx.

En caso de que no se emitan el o los Recibos Electrónicos de Pagos **(REP)** hay 2 opciones:

a) En la página del **SAT** se ingresa una solicitud de conciliación con **"EL PROVEEDOR"** para determinar cuántos **REP** están pendientes y requerir la inmediata entrega de estos comprobantes.
b) Denuncia ante la autoridad fiscal.

El **DT** enviará por correo electrónico semanalmente los comprobantes de pago en formato digital (CLC) al Administrador (a) y al Supervisor (a) del contrato.

QUINTA. LUGAR, PLAZOS Y CONDICIONES DE LA PRESTACIÓN DE LOS SERVICIOS.
La prestación de los servicios, se realizará conforme a los plazos, condiciones y entregables establecidos por **"EL INEA"** en el **"ANEXO ÚNICO",** el cual forma parte del presente contrato.

Los servicios serán prestados en el domicilio señalado en el **"ANEXO ÚNICO"** y fechas establecidas en el mismo.

En los casos que derivado de la verificación se detecten defectos o discrepancias en la prestación del servicio o incumplimiento en las especificaciones técnicas, **"EL PROVEEDOR"** contará con un plazo de **3 DÍAS** para la reposición o corrección, contados a partir del momento de la notificación por correo electrónico y/o escrito, sin costo adicional para **"EL INEA"**.

SEXTA. VIGENCIA.
"LAS PARTES" convienen en que la vigencia del presente instrumento jurídico será del 5 de junio y hasta el 31 de diciembre de 2024.

"LAS PARTES" convienen en que la vigencia del servicio será dentro de los 45 días posteriores a la notificación del fallo y hasta el 31 de diciembre de 2024.

Francisco Márquez 160, Col . Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea

SÉPTIMA. MODIFICACIONES DEL CONTRATO.
"LAS PARTES" están de acuerdo que **"EL INEA"** por razones fundadas y explícitas podrá ampliar el monto o la cantidad de los servicios, de conformidad con el artículo 52 de la **"LAASSP"**, siempre y cuando las modificaciones no rebasen en su conjunto el 20% (veinte por ciento) de los establecidos originalmente, el precio unitario sea igual al originalmente pactado y el contrato esté vigente. La modificación se formalizará mediante la celebración de un Convenio Modificatorio.

"EL INEA", podrá ampliar la vigencia del presente instrumento, siempre y cuando, no implique incremento del monto contratado o de la cantidad del servicio, siendo necesario que se obtenga el previo consentimiento de **"EL PROVEEDOR"**.

De presentarse caso fortuito o fuerza mayor, o por causas atribuibles a **"EL INEA"**, se podrá modificar el plazo del presente instrumento jurídico, debiendo acreditar dichos supuestos con las constancias respectivas. La modificación del plazo por caso fortuito o fuerza mayor podrá ser solicitada por cualquiera de **"LAS PARTES".**

En los supuestos previstos en los dos párrafos anteriores, no procederá la aplicación de penas convencionales por atraso.

Cualquier modificación al presente contrato deberá formalizarse por escrito, y deberá suscribirse por el servidor público de **"EL INEA"** que lo haya hecho, o quien lo sustituya o esté facultado para ello, para lo cual **"EL PROVEEDOR"** realizará el ajuste respectivo de la garantía de cumplimiento, en términos del artículo 91, último párrafo del Reglamento de la **"LAASSP"**, salvo que por disposición legal se encuentre exceptuado de presentar garantía de cumplimiento.

"EL INEA" se abstendrá de hacer modificaciones que se refieran a precios, anticipos, pagos progresivos, especificaciones y, en general, cualquier cambio que implique otorgar condiciones más ventajosas a un proveedor comparadas con las establecidas originalmente.

OCTAVA. GARANTÍA DE LOS SERVICIOS.
Para la prestación de los servicios materia del presente contrato, no se requiere que **"EL PROVEEDOR"** presente una garantía por la calidad de los mismos; sin embargo, los equipos objeto del servicio de arrendamiento tendrán una garantía de 90 días naturales sobre cualquier parte o componente del equipo contados a partir de la fecha de conclusión del contrato.

NOVENA. GARANTÍA(S)
A) CUMPLIMIENTO DEL CONTRATO.
Conforme a los artículos 48, fracción II, 49, fracción I de la **"LAASSP"**, 85, fracción III, 103 de su Reglamento, y 166 de la Ley de Instituciones de Seguros y de Fianzas, **"EL PROVEEDOR"** se obliga a constituir una garantía **divisible**, la cual sólo se hará efectiva en

Francisco Márquez 160, Col . Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea

proporción correspondiente al incumplimiento de la obligación principal, mediante fianza expedida por compañía afianzadora mexicana autorizada por la Comisión Nacional de Seguros y de Fianzas, a favor de **"EL INEA"**, por un importe equivalente al 10% del monto total del contrato, sin incluir Impuesto al Valor Agregado (I.V.A.).

Dicha garantía deberá ser entregada a **"EL INEA"**, a más tardar dentro de los 10 (diez) días naturales posteriores a la firma del presente Contrato.

Si las disposiciones jurídicas aplicables lo permiten, la entrega de la garantía de cumplimiento se podrá realizar de manera electrónica.

En caso de que **"EL PROVEEDOR"** incumpla con la entrega de la garantía en el plazo establecido, **"EL INEA"** podrá rescindir el contrato y dará vista a la Oficina de Representación en **"EL INEA"** para que proceda en el ámbito de sus facultades.

La garantía de cumplimiento no será considerada como una limitante de responsabilidad de **"EL PROVEEDOR"**, derivada de sus obligaciones y garantías estipuladas en el presente instrumento jurídico, y no impedirá que **"EL INEA"** reclame la indemnización por cualquier incumplimiento que pueda exceder el valor de la garantía de cumplimiento.

En caso de incremento al monto del presente instrumento jurídico o modificación al plazo, **"EL PROVEEDOR"** se obliga a entregar a **"EL INEA",** dentro de los 10 (diez días) naturales siguientes a la formalización del mismo, de conformidad con el último párrafo del artículo 91 del Reglamento de la **"LAASSP"**, los documentos modificatorios o endosos correspondientes, debiendo contener en el documento la estipulación de que se otorga de manera conjunta, solidaria e inseparable de la garantía otorgada inicialmente.

Cuando la contratación abarque más de un ejercicio fiscal, la garantía de cumplimiento del contrato, podrá ser por el porcentaje que corresponda del monto total por erogar en el ejercicio fiscal de que se trate, y deberá ser renovada por **"EL PROVEEDOR"** cada ejercicio fiscal por el monto que se ejercerá en el mismo, la cual deberá presentarse a **"EL INEA"** a más tardar dentro de los primeros 10 (diez) días naturales del ejercicio fiscal que corresponda.

Una vez cumplidas las obligaciones a satisfacción, el Administrador (a) del contrato procederá inmediatamente a extender la constancia de cumplimiento de las obligaciones contractuales y dará inicio a los trámites para la cancelación de la garantía cumplimiento del contrato, lo que comunicará a **"EL PROVEEDOR"**.

DÉCIMA. OBLIGACIONES DE "EL PROVEEDOR".
"EL PROVEEDOR", se obliga a:

a) Prestar los servicios en las fechas o plazos y lugares establecidos conforme a lo pactado en el presente contrato y su **"ANEXO ÚNICO"**.

Francisco Márquez 160, Col . Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea

b) Cumplir con las especificaciones técnicas, de calidad y demás condiciones establecidas en el presente contrato y su **"ANEXO ÚNICO"**.

c) Asumir la responsabilidad de cualquier daño que llegue a ocasionar a **"EL INEA"** o a terceros con motivo de la ejecución y cumplimiento del presente contrato.

d) Proporcionar la información que le sea requerida por la Secretaría de la Función Pública y la Oficina de Representación en **"EL INEA"**, de conformidad con el artículo 107 del Reglamento de la **"LAASSP"**.

DÉCIMA PRIMERA. OBLIGACIONES DE "EL INEA".
"EL INEA", se obliga a:

a) Otorgar las facilidades necesarias, a efecto de que **"EL PROVEEDOR"** lleve a cabo en los términos convenidos para la prestación de los servicios objeto del contrato.

b) Realizar el pago correspondiente en tiempo y forma.

c) Extender a **"EL PROVEEDOR"**, por conducto del servidor público facultado, la constancia de cumplimiento de obligaciones contractuales inmediatamente que se cumplan éstas a satisfacción expresa de dicho servidor público para que se dé trámite a la cancelación de la garantía de cumplimiento del presente contrato.

DÉCIMA SEGUNDA. ADMINISTRACIÓN, VERIFICACIÓN, SUPERVISIÓN Y ACEPTACIÓN DE LOS SERVICIOS.
"EL INEA" designa como persona Administradora del presente contrato a la María Dolores Durán Márquez, en su carácter de Subdirectora de Recursos Tecnológicos, con R.F.C. DUMD6808112R5, persona facultada para administrar, dar seguimiento y verificar el debido cumplimiento de las obligaciones contenidas en el contrato, asistir en la formalización del mismo, autorizar la constancia de recepción elaborar la solicitud de liberación de pago y en su caso determinar la aplicación y cálculo de las penas convencionales y deductivas.

Los servicios se tendrán por recibidos previa revisión de la persona Supervisora del presente contrato, el C. Roberto Ramírez Guzmán, Jefe de Departamento de Soporte Técnico, Centro de Datos y Comunicación, con RFC RAGR740522162, será el responsable de auxiliar al administrador en la verificación y revisión del cumplimiento del contrato, establecer los mecanismos de comprobación, supervisión y verificación de los servicios contratados y efectivamente prestados, constatar el cumplimiento de los requerimientos de cada entregable para proceder al pago de la factura, realizar la constancia de recepción y realizar los trámites necesarios para el pago de la factura que presente **"EL PROVEEDOR"**, de acuerdo con las especificaciones establecidas en el **"ANEXO ÚNICO"**.

"EL INEA", a través de la persona Supervisora del contrato, rechazará los servicios, que no cumplan las especificaciones establecidas en este contrato y en su **"ANEXO ÚNICO"**, obligándose **"EL PROVEEDOR"** en este supuesto a realizarlos nuevamente bajo su

Francisco Márquez 160, Col . Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea

responsabilidad y sin costo adicional para **"EL INEA"**, sin perjuicio de la aplicación de las penas convencionales o deducciones al cobro correspondientes.

"EL INEA", a través de la persona Supervisora del contrato, podrá aceptar los servicios que incumplan de manera parcial o deficiente las especificaciones establecidas en este contrato y en su **"ANEXO ÚNICO"**, sin perjuicio de la aplicación de las deducciones al pago que procedan, y reposición del servicio, cuando la naturaleza propia de éstos lo permita.

DÉCIMA TERCERA. DEDUCCIONES.
"EL INEA" aplicará deducciones al pago por el incumplimiento parcial, por atraso o deficiencia, en que incurra **"EL PROVEEDOR"** conforme a lo estipulado en las cláusulas del presente contrato y su **"ANEXO ÚNICO"**, las cuales se calcularan por el **5%** sobre el importe diario de los servicios parciales o deficientes no prestados; igual porcentaje se aplicará en los casos que "EL PROVEEDOR" suspenda el arrendamiento por cualquier causa injustificada, esto es fuera de los casos de fuerza mayor o caso fortuito debidamente acreditado, por cada día natural que suspenda el arrendamiento, independientemente de que no se pagaría arrendamiento por el tiempo que dure la suspensión.

Las cantidades a deducir se aplicarán en el CFDI o factura electrónica que **"EL PROVEEDOR"** presente para su cobro, en el pago que se encuentre en trámite o bien en el siguiente pago.

De no existir pago pendiente, se requerirá a **"EL PROVEEDOR"** que realice el pago de la deductiva a través del esquema e5cinco Pago Electrónico de Derechos, Productos y Aprovechamientos (DPA's), a favor de **"EL INEA"**. En caso de negativa se procederá a hacer efectiva la garantía de cumplimiento del contrato.

Las deducciones económicas se aplicarán sobre la cantidad indicada sin incluir impuestos.

La notificación y cálculo de las deducciones correspondientes, las realizará la persona Administradora del contrato, por escrito o vía correo electrónico a **"EL PROVEEDOR"**.

DÉCIMA CUARTA. PENAS CONVENCIONALES.
En caso que **"EL PROVEEDOR"** incurra en atraso en el inicio de la prestación del servicio objeto del presente contrato, acorde a lo establecido en el **"ANEXO ÚNICO"** el cual forma parte integral de este instrumento jurídico, **"EL INEA"** por conducto de la persona Administradora del contrato aplicará la pena convencional equivalente al **5%** sobre el monto mensual del pago previsto para los equipos no entregados, instalados, configurados y puestos en marcha, conforme a los plazos de entrega de los equipos, por cada día natural de atraso, la misma pena se aplicara en caso de no proporcionar la mesa de ayuda dentro de los 5 días hábiles posteriores contados a partir de la primera entrega de equipo sin exceder el monto de la garantía, de conformidad con este instrumento legal y su **"ANEXO ÚNICO"**.

Francisco Márquez 160, Col . Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea

La persona Administradora del contrato, notificará a **"EL PROVEDOOR"** por escrito o vía correo electrónico, el cálculo de la pena convencional del atraso en el cumplimiento de la obligación de que se trate.

El pago de los servicios quedará condicionado, proporcionalmente, al pago que **"EL PROVEEDOR"** deba efectuar por concepto de penas convencionales por atraso; en el supuesto que el contrato sea rescindido en términos de lo previsto en la Cláusula Vigésima Cuarta de Rescisión, no procederá el cobro de dichas penas ni la contabilización de las mismas al hacer efectiva la garantía de cumplimiento del contrato.

El pago de la pena podrá efectuarse a través del esquema e5cinco Pago Electrónico de Derechos, Productos y Aprovechamientos (DPA's), a favor de **"EL INEA"**; o bien, a través de un comprobante de egreso (**CFDI** de Egreso) conocido comúnmente como Nota de Crédito, en el momento en el que emita el comprobante de Ingreso (Factura o **CFDI** de Ingreso) por concepto de los servicios, en términos de las disposiciones jurídicas aplicables.

El importe de la pena convencional, no podrá exceder el equivalente al monto total de la garantía de cumplimiento del contrato, y serán determinadas en función de los servicios no prestados oportunamente.

"EL PROVEEDOR" quedará obligado ante **"EL INEA"** a responder por la calidad de los servicios, así como de cualquier otra responsabilidad en que hubiera incurrido, en los términos señalados en este instrumento jurídico y en la legislación aplicable.

Cuando **"EL PROVEEDOR"** quede exceptuado de la presentación de la garantía de cumplimiento, en los supuestos previsto en la **"LAASSP"**, el monto máximo de las penas convencionales por atraso que se puede aplicar, será del 20% (veinte por ciento) del monto de los servicios prestados fuera de la fecha convenida, de conformidad con lo establecido en el tercer párrafo del artículo 96 del Reglamento de la **"LAASSP"**.

DÉCIMA QUINTA. LICENCIAS, AUTORIZACIONES Y PERMISOS.
"EL PROVEEDOR" se obliga a observar y mantener vigentes las licencias, autorizaciones, permisos o registros requeridos para el cumplimiento de sus obligaciones.

DÉCIMA SEXTA. PÓLIZA DE RESPONSABILIDAD CIVIL.
Para la prestación de los servicios materia del presente contrato, no se requiere que **"EL PROVEEDOR"** contrate una póliza de seguro por responsabilidad civil del valor del contrato.

DÉCIMA SÉPTIMA. TRANSPORTE.
"EL PROVEEDOR" se obliga bajo su costa y riesgo, a trasportar los bienes e insumos necesarios para la prestación del servicio, desde su lugar de origen, hasta las instalaciones señaladas en el **"ANEXO ÚNICO"** del presente contrato.

DÉCIMA OCTAVA. IMPUESTOS Y DERECHOS.

Francisco Márquez 160, Col . Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea

Los impuestos, derechos y gastos que procedan con motivo de la prestación de los servicios, objeto del presente contrato, serán pagados por **"EL PROVEEDOR"**, mismos que no serán repercutidos a **"EL INEA"**.

"EL INEA" sólo cubrirá, cuando aplique, lo correspondiente al I.V.A., en los términos de la normatividad aplicable y de conformidad con las disposiciones fiscales vigentes.

DÉCIMA NOVENA. PROHIBICIÓN DE CESIÓN DE DERECHOS Y OBLIGACIONES.
"EL PROVEEDOR" no podrá ceder total o parcialmente los derechos y obligaciones derivados del presente contrato, a favor de cualquier otra persona física o moral, con excepción de los derechos de cobro, en cuyo caso se deberá contar con la conformidad previa y por escrito de **"EL INEA"**.

VIGÉSIMA. DERECHOS DE AUTOR, PATENTES Y/O MARCAS.
"EL PROVEEDOR" será responsable en caso de infringir patentes, marcas o viole otros registros de derechos de propiedad industrial a nivel nacional e internacional, con motivo del cumplimiento de las obligaciones del presente contrato, por lo que se obliga a responder personal e ilimitadamente de los daños y perjuicios que pudiera causar a **"EL INEA"** o a terceros.

De presentarse alguna reclamación en contra de **"EL INEA"**, por cualquiera de las causas antes mencionadas, **"EL PROVEEDOR"**, se obliga a salvaguardar los derechos e intereses de **"EL INEA"** de cualquier controversia, liberándola de toda responsabilidad de carácter civil, penal, mercantil, fiscal o de cualquier otra índole, sacándola en paz y a salvo.

En caso de que **"EL INEA"** tuviese que erogar recursos por cualquiera de estos conceptos, **"EL PROVEEDOR"** se obliga a reembolsar de manera inmediata los recursos erogados por aquella.

VIGÉSIMA PRIMERA. CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES.
"LAS PARTES" acuerdan que la información que se intercambie de conformidad con las disposiciones del presente instrumento, se tratarán de manera confidencial, siendo de uso exclusivo para la consecución del objeto del presente contrato y no podrá difundirse a terceros de conformidad con lo establecido en las Leyes General y Federal respectivamente, de Transparencia y Acceso a la Información Pública, Ley General de Protección de Datos Personales en posesión de Sujetos Obligados, y demás legislación aplicable.

Para el tratamiento de los datos personales que **"LAS PARTES"** recaben con motivo de la celebración del presente contrato, deberá de realizarse con base en lo previsto en los Avisos de Privacidad respectivos.

Por tal motivo, **"EL PROVEEDOR"** asume cualquier responsabilidad que se derive del incumplimiento de su parte, o de sus empleados, a las obligaciones de confidencialidad descritas en el presente contrato.

Francisco Márquez 160, Col . Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea

Asimismo **"EL PROVEEDOR"** deberá observar lo establecido en el **"ANEXO ÚNICO"** aplicable a la Confidencialidad de la información del presente Contrato.

VIGÉSIMA SEGUNDA. SUSPENSIÓN TEMPORAL DE LA PRESTACIÓN DE LOS SERVICIOS.

Con fundamento en el artículo 55 Bis de la **"LAASSP"** y 102, fracción II de su Reglamento, **"EL INEA"** en el supuesto de caso fortuito o de fuerza mayor o por causas que le resulten imputables, podrá suspender la prestación de los servicios, de manera temporal, quedando obligado a pagar a **"EL PROVEEDOR"**, aquellos servicios que hubiesen sido efectivamente prestados, así como, al pago de gastos no recuperables previa solicitud y acreditamiento.

Una vez que hayan desaparecido las causas que motivaron la suspensión, el contrato podrá continuar produciendo todos sus efectos legales, si **"EL INEA"** así lo determina; y en caso que subsistan los supuestos que dieron origen a la suspensión, se podrá iniciar la terminación anticipada del contrato, conforme lo dispuesto en la cláusula siguiente.

VIGÉSIMA TERCERA. TERMINACIÓN ANTICIPADA DEL CONTRATO.

"EL INEA" cuando concurran razones de interés general, o bien, cuando por causas justificadas se extinga la necesidad de requerir los servicios originalmente contratados y se demuestre que de continuar con el cumplimiento de las obligaciones pactadas, se ocasionaría algún daño o perjuicio a **"EL INEA"**, o se determine la nulidad total o parcial de los actos que dieron origen al presente contrato, con motivo de la resolución de una inconformidad o intervención de oficio, emitida por la Secretaría de la Función Pública, podrá dar por terminado anticipadamente el presente contrato sin responsabilidad alguna para **"EL INEA"**, ello con independencia de lo establecido en la cláusula que antecede.

Cuando **"EL INEA"** determine dar por terminado anticipadamente el contrato, lo notificará a **"EL PROVEEDOR"** hasta con 30 (treinta) días naturales anteriores al hecho, debiendo sustentarlo en un dictamen fundado y motivado, en el que, se precisarán las razones o causas que dieron origen a la misma y pagará a **"EL PROVEEDOR"** la parte proporcional de los servicios prestados, así como los gastos no recuperables en que haya incurrido, previa solicitud por escrito, siempre que éstos sean razonables, estén debidamente comprobados y se relacionen directamente con el presente contrato, limitándose según corresponda a los conceptos establecidos en la fracción I del artículo 102 del Reglamento de la **"LAASSP"**.

VIGÉSIMA CUARTA. RESCISIÓN.

"EL INEA" podrá en cualquier momento rescindir administrativamente el presente contrato y hacer efectiva la fianza de cumplimiento, cuando **"EL PROVEEDOR"** incurra en incumplimiento de sus obligaciones contractuales, sin necesidad de acudir a los tribunales competentes en la materia, por lo que, de manera enunciativa, más no limitativa, se entenderá por incumplimiento:

Francisco Márquez 160, Col . Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea

a) Contravenir los términos pactados para la prestación de los servicios, establecidos en el presente contrato y su **"ANEXO ÚNICO"**;

b) Transferir en todo o en parte las obligaciones que deriven del presente contrato a un tercero ajeno a la relación contractual;

c) Ceder los derechos de cobro derivados del contrato, sin contar con la conformidad previa y por escrito de **"EL INEA"**;

d) Suspender total o parcialmente y sin causa justificada la prestación de los servicios del presente contrato;

e) No realizar la prestación de los servicios en tiempo y forma conforme a lo establecido en el presente contrato y su **"ANEXO ÚNICO"**;

f) No proporcionar a los Órganos de Fiscalización, la información que le sea requerida con motivo de las auditorías, visitas e inspecciones que realicen;

g) Ser declarado en concurso mercantil, o por cualquier otra causa distinta o análoga que afecte su patrimonio;

h) En caso de que compruebe la falsedad de alguna manifestación, información o documentación proporcionada para efecto del presente contrato;

i) No entregar dentro de los 10 (diez) días naturales siguientes a la fecha de firma del presente contrato, la garantía de cumplimiento del mismo;

j) En caso de que la suma de las penas convencionales o las deducciones al pago, igualan el monto total de la garantía de cumplimiento del contrato y/o alcanzan el 20% (veinte por ciento) del monto total de este contrato cuando no se haya requerido la garantía de cumplimiento;

k) Divulgar, transferir o utilizar la información que conozca en el desarrollo del cumplimiento del objeto del presente contrato, sin contar con la autorización de **"EL INEA"** en los términos de lo dispuesto en la Cláusula Vigésima Primera de Confidencialidad y Protección de Datos Personales del presente instrumento jurídico;

l) Impedir el desempeño normal de labores de **"EL INEA"**;

m) Cambiar su nacionalidad por otra e invocar la protección de su gobierno contra reclamaciones y órdenes de "EL INEA", cuando sea extranjero, y

n) Incumplir cualquier obligación distinta de las anteriores y derivadas del presente contrato.

Francisco Márquez 160, Col . Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea

Para el caso de optar por la rescisión del contrato, **"EL INEA"** comunicará por escrito a **"EL PROVEEDOR"** el incumplimiento en que haya incurrido, para que en un término de 5 (cinco) días hábiles contados a partir del día siguiente de la notificación, exponga lo que a su derecho convenga y aporte en su caso las pruebas que estime pertinentes.

Transcurrido dicho término **"EL INEA"**, en un plazo de 15 (quince) días hábiles siguientes, tomando en consideración los argumentos y pruebas que hubiere hecho valer **"EL PROVEEDOR"**, determinará de manera fundada y motivada dar o no por rescindido el contrato, y comunicará a **"EL PROVEEDOR"** dicha determinación dentro del citado plazo.

Cuando se rescinda el contrato, se formulará el finiquito correspondiente, a efecto de hacer constar los pagos que deba efectuar **"EL INEA"** por concepto del contrato hasta el momento de rescisión, o los que resulten a cargo de **"EL PROVEEDOR"**.

Iniciado un procedimiento de conciliación **"EL INEA"** podrá suspender el trámite del procedimiento de rescisión.

Si previamente a la determinación de dar por rescindido el contrato se realiza la prestación de los servicios, el procedimiento iniciado quedará sin efecto, previa aceptación y verificación de **"EL INEA"** de que continúa vigente la necesidad de la prestación de los servicios, aplicando, en su caso, las penas convencionales correspondientes.

"EL INEA" podrá determinar no dar por rescindido el contrato, cuando durante el procedimiento advierta que la rescisión del mismo pudiera ocasionar algún daño o afectación a las funciones que tiene encomendadas. En este supuesto, **"EL INEA"** elaborará un dictamen en el cual justifique que los impactos económicos o de operación que se ocasionarían con la rescisión del contrato resultarían más inconvenientes.

De no rescindirse el contrato, **"EL INEA"** establecerá con **"EL PROVEEDOR"**, otro plazo, que le permita subsanar el incumplimiento que hubiere motivado el inicio del procedimiento, aplicando las sanciones correspondientes. El convenio modificatorio que al efecto se celebre deberá atender a las condiciones previstas por los dos últimos párrafos del artículo 52 de la **"LAASSP"**.

No obstante, de que se hubiere firmado el convenio modificatorio a que se refiere el párrafo anterior, si se presenta de nueva cuenta el incumplimiento, **"EL INEA"** quedará expresamente facultada para optar por exigir el cumplimiento del contrato, o rescindirlo, aplicando las sanciones que procedan.

Si se llevara a cabo la rescisión del contrato, y en el caso de que a **"EL PROVEEDOR"** se le hubieran entregado pagos progresivos, éste deberá de reintegrarlos más los intereses correspondientes, conforme a lo indicado en el **artículo 51,** párrafo cuarto de la **"LAASSP"**.

Los intereses se calcularán sobre el monto de los pagos progresivos efectuados y se computarán por días naturales desde la fecha de su entrega hasta la fecha en que se pongan efectivamente las cantidades a disposición de **"EL INEA"**.

Francisco Márquez 160, Col . Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea

VIGÉSIMA QUINTA. RELACIÓN Y EXCLUSIÓN LABORAL.
"EL PROVEEDOR" reconoce y acepta ser el único patrón de todos y cada uno de los trabajadores que intervienen en la prestación del servicio, deslindando de toda responsabilidad a **"EL INEA"** respecto de cualquier reclamo que en su caso puedan efectuar sus trabajadores, sea de índole laboral, fiscal o de seguridad social y en ningún caso se le podrá considerar patrón sustituto, patrón solidario, beneficiario o intermediario.

"EL PROVEEDOR" asume en forma total y exclusiva las obligaciones propias de patrón respecto de cualquier relación laboral, que el mismo contraiga con el personal que labore bajo sus órdenes o intervenga o contrate para la atención de los asuntos encomendados por **"EL INEA"**, así como en la ejecución de los servicios.

Para cualquier caso no previsto, **"EL PROVEEDOR"** exime expresamente a **"EL INEA"** de cualquier responsabilidad laboral, civil o penal o de cualquier otra especie que en su caso pudiera llegar a generarse, relacionado con el presente contrato.

Para el caso que, con posterioridad a la conclusión del presente contrato, **"EL INEA"** reciba una demanda laboral por parte de trabajadores de **"EL PROVEEDOR"**, en la que se demande la solidaridad y/o sustitución patronal a **"EL INEA"**, **"EL PROVEEDOR"** queda obligado a dar cumplimiento a lo establecido en la presente cláusula.

VIGÉSIMA SEXTA. DISCREPANCIAS.
"LAS PARTES" convienen que, en caso de discrepancia entre la convocatoria y el contrato, prevalecerá lo establecido en la convocatoria, de conformidad con el artículo 81, fracción IV del Reglamento de la **"LAASSP"**.

VIGÉSIMA SÉPTIMA. CONCILIACIÓN.
"LAS PARTES" acuerdan que para el caso de que se presenten desavenencias derivadas de la ejecución y cumplimiento del presente contrato podrán someterse al procedimiento de conciliación establecido en los artículos 77, 78 y 79 de la **"LAASSP"**, 126 al 136 de su Reglamento.

VIGÉSIMA OCTAVA. DOMICILIOS.
"LAS PARTES" señalan como sus domicilios legales para todos los efectos a que haya lugar y que se relacionan en el presente contrato, los que se indican en el apartado de Declaraciones, por lo que cualquier notificación judicial o extrajudicial, emplazamiento, requerimiento o diligencia que en dichos domicilios se practique, será enteramente válida, al tenor de lo dispuesto en el Título Tercero del Código Civil Federal.

VIGÉSIMA NOVENA. LEGISLACIÓN APLICABLE.
"LAS PARTES" se obligan a sujetarse estrictamente para la prestación de los servicios objeto del presente contrato a todas y cada una de las cláusulas que lo integran, su **"ANEXO ÚNICO"** que forma parte integral del mismo, a la **"LAASSP"**, su Reglamento; Código Civil Federal; Ley Federal de Procedimiento Administrativo, Código Federal de Procedimientos Civiles; Ley Federal de Presupuesto y Responsabilidad Hacendaria y su Reglamento, Ley General de Comunicación Social.

Francisco Márquez 160, Col . Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea

TRIGÉSIMA. JURISDICCIÓN.
"LAS PARTES" convienen que, para la interpretación y cumplimiento de este contrato, así como para lo no previsto en el mismo, se someterán a la jurisdicción y competencia de los Tribunales Federales con sede en la Ciudad de México, renunciando expresamente al fuero que pudiera corresponderles en razón de su domicilio actual o futuro.

"LAS PARTES" manifiestan estar conformes y enterados de las consecuencias, valor y alcance legal de todas y cada una de las estipulaciones que el presente instrumento jurídico contiene, por lo que lo ratifican y firman en las fechas especificadas en cada firma, dentro de los 15 días establecidos en la "LAASSP".

POR
"EL INEA"

NOMBRE	CARGO	RFC
MARÍA ISABEL MONTOYA OBREGÓN	**APODERADA LEGAL Y TITULAR DE LA UNIDAD DE ADMINISTRACIÓN Y FINANZAS.**	**MOOI570119MR9**
MARÍA DOLORES DURÁN MÁRQUEZ	**SUBDIRECTORA DE RECURSOS TECNOLÓGICOS**	**DUMD6808112R5**
ROBERTO RAMÍREZ GUZMÁN.	**JEFE DE DEPARTAMENTO DE SOPORTE TÉCNICO, CENTRO DE DATOS Y COMUNICACIÓN**	**RAGR740522162**

POR
"EL PROVEEDOR"

NOMBRE	R.F.C.
REISCOM, S.A. DE C.V.	**REI0409133L4**

Francisco Márquez 160, Col . Condesa, CP. 06140, Alcaldía Cuauhtémoc, CDMX.
Tel: (55) 5241 2700 www.gob.mx/inea

Cadena original:

cf10d3eb4b80f1fdd74306ab6e6152f1822b19451b959eba448ba2d0b2beb22b

Firmante: MARIA DOLORES DURAN MARQUEZ
RFC: DUMD6808112R5

Número de Serie: 00001000000504622569
Fecha de Firma: 19/06/2024 13:54

Certificado:

MIIGQDCCBCigAwIBAgIUMDAwMDEwMDAwMDA1MDQ2MjI1NjkwDQYJKoZIhvcNAQELBQAwggGEMSAwHgYDVQQDDBdBVVRPUklEQUQgQ0VSVElGSUNBRE9SQTEuMCwGA1UECgwlU0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEaMBgGA1UECwwRU0FULUlFUyBBdXRob3JpdHkxKjAoBgkqhkiG9w0BCQEWG2NvbnRhY3RvLnRlY25pY29Ac2F0LmdvYi5teDEmMCQGA1UECQwdQVYuIEhJREFMR08gNzcsIENPTC4g
R1VFUlJFUk8xDjAMBgNVBBEMBTA2MzAwMQswCQYDVQQGEwJNWDEZMBcGA1UECAwQQ0lVREFEIERFIE1FWElDTzETMBEGA1UEBwwKQ1VBVUhURU1PQzEVMBMGA1UELRMMU0FUOTcwNzAxTk4zMVwwWgYJKoZIhvcN
AQkCE01yZXNwb25zYWJsZTogQURNSU5JU1RSQUNJT04gQ0VOVFJBTCBERSBTRVJWSUNJT1MgVFJJQlVUQVJJT1MgQUwgQ09OVFJJQlVZRU5URTAeFw0yMDA3MjkyMTE0NDFaFw0yNDA3MjkyMTE1MjFaMIHcMSQw
IgYDVQQDExtNQVJJQSBET0xPUkVTIERVUkFOIE1BUlFVRVoxJDAiBgNVBCkTG01BUklBIERPTE9SRVMgRFVSQU4gTUFSUVVFWjEkMCIGA1UEChMbTUFSSUEgRE9MT1JFUyBEVVJBTiBNQVJRVUVaMQswCQYDVQQG
EwJNWDEmMCQGCSqGSIb3DQEJARYXbWxvbGl0YS5kdXJhbkBnbWFpbC5jb20xFjAUBgNVBC0TDURVTUQ2ODA4MTEyUjUxGzAZBgNVBAUTEkRVTUQ2ODA4MTFNREZSUkwwNTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAIqg/5WdonVQdzb4A0tvQBNa3GXqAX8Ksh4pXBZ8lr2VlctuUyAC75h+dLvs2BHqZ5uxJ8smpLvGKRTUBPmRt4dHbIB3WQKs7SA2704/IPXoDh0cif3km57kY0vb1GHjyY0PmUhfOd5ocJhzMM17
LbHZ4dMZW0FiIYn8ORr1e3roRbUvAyWg1GRcGB+Pceafsbh/kM0ZK0wqnCR0EUwKZkiVDDAWwV8nK3aUqKhISJd6IMHAqN3nGmpRwQxoNiCquyU1FhFMNVZEHQa/pYPzZP2BUsKGbtp1wAsma1myQCey0hJtErxL
dm9MhemLKmkbPWVqyrecu8rtKDrc/BD9rR8CAwEAAaNPME0wDAYDVR0TAQH/BAIwADALBgNVHQ8EBAMCA9gwEQYJYIZIAYb4QgEBBAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMEBggrBgEFBQcDAjANBgkqhkiG
9w0BAQsFAAOCAgEAMCrm3k/olAiKE3xgNG4osErroU6GqT6qeSLoyGhCVGZWBaD2avhc97I6igbMTgJycSOQ5yUdSjgN05wkz1q/k2pr5H56kjAxlZqan1xw/sgpjMxiQivgikR5a0A/qX5kdcIpvsicqA/W0+ME
091zF9vfeDmx/TFZaG8vZbMI0ye+7v7vgacf4prx8+0/z77OUOAofLbVKgTxZKRCoIwjpg3HWBl1G0ZeKEs3XFIQfedr/17rkQzePXhnljM2vooD15P27tg6TvJUwpb0Oh3KRUQerjvooibPFCUFRyidpe2CACMb
5eLv9T3YWL7/dYqropSuwREs7FoTArIRaZVx5ktibRKLDNMY0D0VB9ZG5wzRe9cIUvxmDcIM+s28mchFAhUD4JT/l+W6zbJt8mOuTS2csLDYAn9T56NCxTa+XzWHjCP6QWFITwoPzLjJvPp3sLYiLVXauR/Saqzp
/DWnR4/HLftqRXjKu763MiKyHsrUXPkxXeXwMerxdYaSIPyFMsmldVjNRhDcksr0wiFM2j/4vt6cx7KsWmbfWFfQRlVdtPzTTOb8ERDxSLJMZH0FjyDnSwICuaxF8zti/kw/wHrXtxBgAyZbifdVb4hxgojshRAc
jFZvkdTWVvJ5rPG/YzBOfkFLwRAU3N/XO6hBOM6FOdJsjFDMkqP1qvvU0FQ=

Firma:

dEdxPZ5Eg5rI8szL/MxWem0FJSuzMOQYIxP503v3OY5zdyPEIJZvIbVnxXt+6cAgJfCQf2KRhMs+cYENnafKjR8RIsoJ2PC84eKHMCzzgWqm8NFGKxpYg+Bu7v0anADQd1Vshirn7bP9DLQ3FOeFWlXsM2nxDbGI
GGTRXkBRsc8q8OAA0xuINlCXH+b6XsZ9z6Su3wucMBqwEr0F9NfeMF0GTryDOYDp69ABsYJExFIAZA7TRuRfY+cJUZtpzkN8jTMBcLrE0yu7FlkfEBfqgNKfhgiiNWAg70fpXzjm+zVQS/Ry7R6afnA/o2nsI4YX
9TPTL5czU7O2easzogo9ug==

Firmante: ROBERTO RAMIREZ GUZMAN
RFC: RAGR740522162

Número de Serie: 00001000000519242866
Fecha de Firma: 19/06/2024 14:00

Certificado:

MIIGLTCCBBWgAwIBAgIUMDAwMDEwMDAwMDA1MTkyNDI4NjYwDQYJKoZIhvcNAQELBQAwggGEMSAwHgYDVQQDDBdBVVRPUklEQUQgQ0VSVElGSUNBRE9SQTEuMCwGA1UECgwlU0VSVklDSU8gREUgQURNSU5JU1RS
QUNJT04gVFJJQlVUQVJJQTEaMBgGA1UECwwRU0FULUlFUyBBdXRob3JpdHkxKjAoBgkqhkiG9w0BCQEWG2NvbnRhY3RvLnRlY25pY29Ac2F0LmdvYi5teDEmMCQGA1UECQwdQVYuIEhJREFMR08gNzcsIENPTC4g
R1VFUlJFUk8xDjAMBgNVBBEMBTA2MzAwMQswCQYDVQQGEwJNWDEZMBcGA1UECAwQQ0lVREFEIERFIE1FWElDTzETMBEGA1UEBwwKQ1VBVUhURU1PQzEVMBMGA1UELRMMU0FUOTcwNzAxTk4zMVwwWgYJKoZIhvcN
AQkCE01yZXNwb25zYWJsZTogQURNSU5JU1RSQUNJT04gQ0VOVFJBTCBERSBTRVJWSUNJT1MgVFJJQlVUQVJJT1MgQUwgQ09OVFJJQlVZRU5URTAeFw0yMzA0MTkwMzQ4MjZaFw0yNzA0MTkwMzQ5MDZaMIHJMR8w
HQYDVQQDExZST0JFULRPIFJBTUlSRVogR1VaTUFOMR8wHQYDVQQpExZST0JFULRPIFJBTUlSRVogR1VaTUFOMR8wHQYDVQQKExZST0JFULRPIFJBTUlSRVogR1VaTUFOMQswCQYDVQQGEwJNWDEiMCAGCSqGSIb3
DQEJARYTcm9iZXIwMUBob3RtYWlsLmNvbTEWMBQGA1UELRMNUkFHUjc0MDUyMjE2MjEbMBkGA1UEBRMSUkFHUjc0MDUyMkhERk1aQjAzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAjsAmsuB5b98B
6axBeofiAyDEEz1nSXCT7FYpy1l3CcfT3borDW/fBVIRaFkkpSJy8aMnEuzNyThZTJrdKIi/YvNdh9Oczutd29tUNZrgUmN/xRo7ACpdVD4j9sWpaXLUmoXosJaEMB52NfSyqdiNBqCiuFjSoHtRPCw4ip0dmUdv
VoTaTvllTBLAVfC2ga1ApQ3xENvyCYpTY4fEFVfGiDLx+esPg69OT8FN6eU1GzRvVixyhFHath1Kg27bTq2rYp1CA7tBEfdgvtWRw/aeBjV+1EqwUtSbMDFXIHRD0ZvLFkJyWzZfoNHchQKAhpx4f8C5W8pad/Lt
CnrAyKrW6wIDAQABo08wTTAMBgNVHRMBAf8EAjAAMAsGA1UdDwQEAwID2DARBglghkgBhvhCAQEEBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwQGCCsGAQUFBwMCMA0GCSqGSIb3DQEBCwUAA4ICAQB8+NwW4Y2o
T83vPUquDBSb/XB0sLXVrxuyNtkGQ7EqpyJJvN/tR9CPKE4fOSvOPnYgCfdmJnjSiph6IRUizwBKpK1oLjCy0w913PFWt2YgBWaRlqv+3j34LEsj0Sb425Jeiwsq2Tkz+yr7Rjws1es1NOhj4UUYRilHdJDtbRlr
MNvXA9pLYO2TSvhdJfXkzw5erl1N0T9b2yWUvcb1IPr48VQ/WCXzllgL/x/XQUXvhyw3v/oKy7QdvrDpAY0wAkBTwKPpULISdqnT9WNclo6NPgiILb4V9QWJBL0xC/Z1eidNH0hSm7oFoAwAY9p/QH61so7civfD
2XnFZ7tuZ1bKL8xzHgRBjAUJ8Y1BcKyhCos+qTmDHsgjAqmB9DqtICD/Fm9NFzD2UY9Vd3qA9UrSnAi4kD68NXV3YZIn533bD4qeJSVAvrogYbt9E+0FIJmp8j7H2wfVPKCyvoCmAUzUvKiwjBO/YDXJRCz3RPS3
AYycMwCKWuxoTcngtYFDLhlfmBS+SyeDXP0yoUMIHzZaMKGrwWulhtzRXjE/QgMklZ1MVXNj/CxxtnqTsCKFMFjaLH9b502ZtgfDiNe8n/E9jfFQVbC5QTgyYBmEhrMa827yk2ZeSkpN8xEkfADvIj2Lp4pbqQKl
QnOy0iDoMs/cf5BpHKQ9VnyFFS7ek7U9Lw==

Firma:

TjFxvOukftbHZUWEXD7Cpog1R2Tr72Qo91rnk0v4l3Gwlw0oPbo7kZUz++xNLdPyTfI7iHu6fYwwYirixLWFd0VcZrHqM1g+bkzUnLS8P1KaMSM3S8dMXRp29vAVQwDpyW0WOIsIjz5CQ9AaMiYAG9g21RYxdC6a
J29PXj9em2QJ2dUTuhqmH57WrUl8GFivgJG2bTDnwd058Mu1iJFwtERf+DYWQwkGzSfawQqfAvCFC2sZxwqhGHJ5JUiHLedomfXuhOGzNJRK+f4z7UGL/PxpQns0c3KXfNQqz8kRUAf7NfR1RH8DCWK5JeTFMp2w
k8MoCEL25eFLFFhXqoKqJg==

Firmante: MARIA ISABEL MONTOYA OBREGON
RFC: MOOI570119MR9

Número de Serie: 00001000000705833739
Fecha de Firma: 19/06/2024 14:21

Certificado:

MIIGVTCCBD2gAwIBAgIUMDAwMDEwMDAwMDA3MDU4MzM3MzkwDQYJKoZIhvcNAQELBQAwggGVMTUwMwYDVQQDDCxBQyBERUwgU0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEuMCwGA1UECgwl
U0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEaMBgGA1UECwwRU0FULUlFUyBBdXRob3JpdHkxMjAwBgkqhkiG9w0BCQEWI3NlcnZpY2lvc2FsY29udHJpYnV5ZW50ZUBzYXQuZ29sLm14MSYw
JAYDVQQJDB1Bdi4gSGlkYWxnbyA3NywgQ29sLiBHdWVycmVybzEOMAwGA1UEEQwFMDYzMDAxCzAJBgNVBAYTAk1YMQ0wCwYDVQQIDARDRE1YMRMwEQYDVQQHDApDVUFVSFRFTU9DMRUwEwYDVQQtEwxTQVQ5NzA3
MDFOTjMxXDBaBgkqhkiG9w0BCQITTXJlc3BvbnNhYmxlOiBBRE1JTklTVFJBQ0lPTiBDRU5UUkFMIERFIFNFUlZJQ0lPUyBUUklCVVRBUklPUyBBTCBDT05UUklCVVlFTlRFMB4XDTI0MDMxNjAwNTQ1OFoXDTI4
MDMxNjAwNTUzOFowgeAxJTAjBgNVBAMTHE1BUklBIElTQUJFTCBNT05UT1lBIE9CUkVHT04xJTAjBgNVBCkTHE1BUklBIElTQUJFTCBNT05UT1lBIE9CUkVHT04xJTAjBgNVBAoTHE1BUklBIElTQUJFTCBNT05U
T1lBIE9CUkVHT04xCzAJBgNVBAYTAk1YMScwJQYJKoZIhvcNAQkBFhhtaW1vbnRveWFAcHJvZGlneS5uZXQubXgxFjAUBgNVBC0TDU1PT0k1NzAxMTlNUjkxGzAZBgNVBAUTEk1PT0k1NzAxMTlNVlpOQlMwNDCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJjLYfxiWvGNp4L5lwLCEz/CKUKu48OPcX6388nSy1Qm420bgmR1b2wQT8reMFY59W/po0JSZVtEHauL9CjEXMl4YAF40t+eFDQqfCHYF7fUdkHJIQuTNhtE
cVC8zBF5/KlY/JOKuPvizOZkOQ2xGT5dvdvN2TWBpWXhHy3ELB6q8RHSHD1r9mYsppMpBOO7jbN+tr0G1+Y8taXNPMFh/jdCuvqcJ9H5zYJ/p1MSBGA3vzKBZ9tKhf+qwbvH6rqyow+g6MAs1nBDirwINVqZZ59j
TXnDm2XfIWjApSUL56FBD33T1XSCr3qtoxYLGskr1NQHdLZNRs2XLZHCbF5NticCAwEAAaNPME0wDAYDVR0TAQH/BAIwADALBgNVHQ8EBAMCA9gwEQYJYIZIAYb4QgEBBAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUF
BwMEBggrBgEFBQcDAjANBgkqhkiG9w0BAQsFAAOCAgEAibVRL5M43oQj9FcLN1z5t8i3GppxZ73lxikc+gZM3QdTsNyhRjOOzGj/m39Wbz8QA1TrleNMP+IBbJcWL+6albRkvyY+4AmrSeD1iGJpZ0tptWDMJQpn
EpmU+ZCH69r/2O1UDE+KrUvVB8nptaLxgcpj2qZSWOKp612gS6LE/vbI6Mu38Qk3ABu1p2fID26fen0C/xghNOjgYv9EK3m89TW4F/RzfQCiummCmbO2cVX4dziALrJAJFu29UuafsPw6EaFvqWgIQUWY9ujONfo
l58Iwj1FcazJ//NHJM4ZdYICHLBaWk6r0PjtN2MJxVc95vIoOPi3oNyJMfRONhMvf40TMDxSDBE/j3+dw5GRJVv2+OHUttGpIZs9pN7+S5D4IUz8rNx6pmtXdIf5/mv3vQeW9yV7VFkCaElsoUIbDcrcmvqlFyTN
/jQS9vHAymZ7S70P8xX5zL9Q3jXXfX7lnWrd5dyGCi+eDfV/w7gQlrwJrX8gVOhoRGygcsV1lwjuE+WRitxgQvlXo7r3S97jdgryaKS6QIAqqlLEiu9gqN9sgdf+bLc7IP8QuKQUMKtxYhjVpfwaWwJKsOXjvDbo
5die//0mU70kDp/Dzr7r4jViJPV2/Fh6vixXQIT9ZA1QkRVSvLjNmjH3s/F31ArQ7P0wDscGDK3u4OGuHnbEXPw=

Firma:

T+WUd90m/+OaiJkJ50KAGhw3ntGBpnEPJVHU6CQyvBF3Ch2CZudd0m1++hi/jjtXwdR0r/JytEzmula8Yb+UhZpZ60Rlz4Yxz2XxoLzoJyhW7HN/OJAv/5DHrEVeca1gUgLKX5HKvj+441dEl76AyFKs1/NhzmyS6kalhLmPdi9sXoHXkUgfuUFWKT+Tdx+eyvZMH2vC3vIwGojGRcu9aljr1WRJz8pIVM1HQW3EXxtS8nBpEvvOjspkzsZRcKLC27whoKCBgPaLLV65Yyw5wZT5tZUTi1LgCWGFJfVZosuFILu7pIfGesjmsJIeflHmVCXTJz1lbHuf5wZp3mBwHw==

Firmante: REISCOM SA DE CV
RFC: REI0409133L4

Número de Serie: 00001000000508265535
Fecha de Firma: 19/06/2024 14:28

Certificado:

MIIGLjCCBBagAwIBAgIUMDAwMDEwMDAwMDA1MDgyNjU1MzUwDQYJKoZIhvcNAQELBQAwggGEMSAwHgYDVQQDDBdBVVRPUklEQUQgQ0VSVElGSUNBRE9SQTEuMCwGA1UECgwlU0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEaMBgGA1UECwwRU0FULUlFUyBBdXRob3JpdHkxKjAoBgkqhkiG9w0BCQEWG2NvbnRhY3RvLnRlY25pY29Ac2F0LmdvYi5teDEmMCQGA1UECQwdQVYuIEhJREFMR08gNzcsIENPTC4gR1VFUlJFUk8xDjAMBgNVBBEMBTA2MzAwMQswCQYDVQQGEwJNWDEZMBcGA1UECAwQQ0lVREFEIERFIE1FWElDTzETMBEGA1UEBwwKQ1VBVUhURU1PQzEVMBMGA1UELRMMU0FUOTcwNzAxTk4zMVwwWgYJKoZIhvcNAQkCE01yZXNwb25zYWJsZTogQURNSU5JU1RSQUNJT04gQ0VOVFJBTCBERSBTRVJWSUNJT1MgVFJJQlVUQVJJT1MgQUwgQ09OVFJJQlVZRU5URTAeFw0yMTA3MjAyMjEyMjRaFw0yNTA3MjAyMjEzMDRaMIHKMRkwFwYDVQQDExBSRUlTQ09NIFNBIERFIENWMRkwFwYDVQQpExBSRUlTQ09NIFNBIERFIENWMQswCQYDVQQGEwJNWDEjMCEGCSqGSIb3DQEJARYUam11cmlsbG9AcmVpc2NvbS5jb20xJTAjBgNVBC0THFJFSTA0MDkxMzNMNCAvIFJPTUE1NTEyMDc3NzQxHjAcBgNVBAUTFSAvIFJPWE01NTEyMDdIREZKWE4wODCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIPeoKFJe1Oh7KZumcNFJLsDzMFGY+ASa8BEIjccp7WWy9Btxvvrxj1pvr8siTRV0Zb3mVtn0TJLk/q9pIALQ9Q4AUEvF1w+ADqEz5aKJ65DdqGnNubP9ZYZRjpMBks54NzPRUzlRq8OPatGR18fJWwQovjUKO2nPA3LbnAyWo757wU0BUKhUkl/+QwHHCoSasKkyed15PQi1tk46Tje+L9wVCA17AjGs/j681O2nnrAsBSarjTkRS2+VOxanariqcJYTdjvcrmmKSqXB5Gc/+EGEU9VDtGlQiXv7W/yQIZGCLOZfIIhWE0+FHApFviBo4Cot3YkaNn19/17eifKAekCAwEAAaNPME0wDAYDVR0TAQH/BAIwADALBgNVHQ8EBAMCA9gwEQYJYIZIAYb4QgEBBAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMEBggrBgEFBQcDAjANBgkqhkiG9w0BAQsFAAOCAgEAW1xKvTBFn7R560BPDW6a/7OU59IfJYzVVZ3CV3dDvy4XmQcRuSWdmU02/dUquDt9eTv9OOxyyr094es1mFkZyQC+j4QhZzzgETgjvRgaNyq0HRu9scVWD8rCInsc1EtEkRQN79HOT8Ky7Hc76WVA3RaPcR7Pv0XzH0R33B/CJgG/TN0BhWJFHFTE2qDTXfdU9JRhwbBI5w0W6e369ZesBfx3oZ1iEBV2IeWVDR6bPiLjjcAKh1ZVejyumKBIHVoiFoKvQSsjZiTNjxBfai2zgFHF5P+JDUukUad4dLOXplOetUFQ2lHze/oX2JJr6M7NY6IhcvAnz6mIbwkHP35GMBmhZezX+IMlVU4mw+x1mZjLW1VB1G3c61pM6U4Qs+s4mpUz1Lo/Ln8Sk+StM6Yjcyzmf34+ntKqfSucTiAanGn3SXrL4IByHI+uZx/usc8vSvqpwhbGjIt4rQN58P6XlAszCBTLUOuxuINu8ekxPL+U3Skwc10zagf+rVvdwZVKzLVwvm0KmatFPjqmc4U1OoRazi2plLTtydg3OHYAWUrza62fPFwpFe1MRUt12O6E0IZlwa/XxwokvMbJBYhfHc1mMgWkTOMY3H0RM0H7RwQeGYR/sMV7XmO5fWg2Pw38WP1+MglTc4Bq+vWX2ouAJz1o89Z4UeSjyDiVngC8rr0=

Firma:

TmNTyeztgthw0onANJx5wCt+vi5tsPXsv4CSUSs6sArbsT296fd9b614OYF+v91/6kSUUvwu2cOVlT14grqcPbDs5xBFiTBhB68tQjJyFr87q0eoLFckTFxq5C8K6c99cnX7+FfYooJZO3oiU0cuNtmaK+fXN9R+WPVjpPb+GcSonTBlj6P2jhFJN3Ko1UxYQfavsghuznuiqzEfGnRuWpfsMPxVD5whCczlfUMvR3CD5xk9pMk+cGy6dDlk1JJOJQRDR1JZIYpbWb2jxOt1ykwIH+Zc8+dSId24+wltb+UqJFtJsVJGV2ONLV1Tfe1sE6dYBmX4+YMdJqkGlCdnTw==

Vanguardia Tecnológica Para Su Empresa

Instituto Nacional para la Educación de los Adultos
Invitación a cuando menos Tres Personas
Procedimiento No. IA-11-MDA-011MDA001-N-59-2024
Nombre del licitante: REISCOM, S.A. DE C.V.
Fecha: 29 de mayo de 2024

FORMATO A-2.

FORMATO DE PROPOSICIÓN ECONÓMICA

Ciudad de México, 29 de mayo de 2024,

HOJA 1 DE 1

RAZÓN SOCIAL: REISCOM, S.A. DE C.V.

DOMICILIO FISCAL: ATLAPULCO NO. 6A, COL. VERGEL DEL SUR, ALACLDÍA DE TLALPAN, C.P. 14340

R.F.C.: REI0409133L4 **TELÉFONO: 55 52643871**

CORREO ELECTRÓNICO: jmurillo@reiscom.com

Partida	Producto	Cantidad	Costo unitario mensual	Costo total (junio a diciembre 2024)
1	Terminal IP básica	195	$ 935.00	$929,390.00
	Terminal IP ejecutiva	85	$ 1910.00	$534,800.00
	Servicio de tarificación telefónica para 649 extensiones	1	$13,250.00	$92,750.00
			SUBTOTAL	$1,556,940.00
			I.V.A.	$249,110.40
			TOTAL	$1,806,050.40
Importe con letra: (UN MILLÓN OCHOCIENTOS SEIS MIL CINCUENTA PESOS 40/100 M.N.) I.V.A. INCLUIDO				

Firma:
Nombre: FRANCISCO JAVIER MURILLO PANTOJA
Cargo: REPRESENTANTE LEGAL

Vanguardia Tecnológica Para Su Empresa

Instituto Nacional para la Educación de los Adultos
Invitación a cuando menos Tres Personas
Procedimiento No. IA-11-MDA-011MDA001-N-59-2024
Nombre del licitante: REISCOM, S.A. DE C.V.
Fecha: 29 de mayo de 2024

ANEXO 1
(Especificaciones Técnicas)

SERVICIO DE ARRENDAMIENTO DE EQUIPO PARA TELEFONÍA IP **UNIDAD DE ADMINISTRACIÓN Y FINANZAS** **SUBDIRECCIÓN DE RECURSOS TECNOLÓGICOS**	
ÁREA REQUIRENTE	Subdirección de Recursos Tecnológicos
NOMBRE DEL TITULAR DEL ÁREA REQUIRENTE Y RESPONSABLE DE ADMINISTRAR Y SUPERVISAR EL CUMPLIMIENTO DEL CONTRATO	Titular del Área Requirente y Administradora del Contrato. María Dolores Durán Márquez Subdirectora de Recursos Tecnológicos Supervisor del Contrato Roberto Ramírez Guzmán Jefe del Departamento de Soporte Técnico, Centro de Datos y Comunicaciones
% PENALIZACIÓN	**Penas convencionales** En el arrendamiento: Reiscom, S.A. de C.V. se obliga a pagar al INEA una pena convencional del 5% sobre el monto mensual del pago previsto para los equipos no entregados, instalados, configurados y puestos en marcha, conforme a lo descrito en el numeral 15 del presente anexo técnico por cada día natural de atraso. La misma pena se aplicará en el caso de no proporcionar la mesa de ayuda dentro de los 5 días hábiles posteriores contados a partir de la primera entrega de equipo. El total de la pena convencional no podrá exceder el monto de la garantía de cumplimiento sin considerar el impuesto al valor agregado (I.V.A), de conformidad con lo establecido en el artículo 53 de la LAASSP. En los entregables: Reiscom, S.A. de C.V. se obliga a pagar al INEA una pena convencional por no presentar los entregables mensuales en los plazos establecidos en el numeral 11 del presente anexo técnico. Dicha pena será del 5% del valor del costo mensual del arrendamiento del equipo, por cada día natural de atraso. El total de la pena convencional no podrá exceder el monto de la garantía de cumplimiento sin considerar el impuesto del valor agregado (I.V.A), de conformidad con lo establecido en el artículo 53 de la LAASSP.
% DE DEDUCCIÓN	Se aplicará una deductiva al Proveedor por el cumplimiento parcial o deficiente en el arrendamiento. Dicha deductiva será del 5%, sobre el monto de la facturación del mes inmediato anterior correspondiente al equipo que no sea sustituido o reparado en los términos y plazos establecidos en el presente anexo por cada día natural de atraso. Lo anterior, de conformidad en lo establecido en el artículo 53 bis de la LAASSP.

	Igual porcentaje, se aplicará como deductiva en los casos que Reiscom, S.A. de C.V. suspenda el arrendamiento por cualquier causa injustificada, esto es fuera de los casos de fuerza mayor o caso fortuito debidamente acreditado y documentado en términos de la normatividad aplicable, por cada día natural que suspenda el arrendamiento, independientemente de que no se pagaría arrendamiento por el tiempo que dure la suspensión. En caso de que los conceptos en los que subsistan el cumplimiento parcial o la deficiencia sean equivalentes al importe de la garantía otorgada por Reiscom, S.A. de C.V. del arrendamiento, el Administrador del Contrato podrá optar por cancelar total o parcialmente el arrendamiento aplicando la pena convencional máxima al Proveedor, lo anterior, en términos del artículo 100 del Reglamento de la Ley antes citada, o bien, optar por rescindir el contrato en término de la Ley.		
TIPO DE GARANTÍA	**DIVISIBLE** [ ]	**INDIVISIBLE** [ ]	
OTRAS GARANTÍAS QUE SE DEBERÁN DE CONSIDERAR, INDICAR EL O LOS TIPOS DE GARANTÍA O DE RESPONSABILIDAD CIVIL SEÑALANDO VIGENCIA	No aplica	**PARTIDA PRESUPUESTAL**	32301
PERIODO DE GARANTÍA DEL SERVICIO	Los equipos objeto del servicio de arrendamiento tendrán una garantía de 90 días naturales sobre cualquier parte o componente del equipo contados a partir de la fecha de conclusión del contrato; en el entendido de que a la conclusión del contrato de arrendamiento deberá estar formalizada la donación de los equipos al INEA y aplicará la garantía establecida.	**PLAZO PARA LA NOTIFICACIÓN Y REPOSICIÓN DEL BIEN O SERVICIO.**	Conforme al anexo técnico
REQUIERE PRUEBAS	No	**REQUIERE MUESTRA**	No
MÉTODO PARA EJECUTAR LA PRUEBA Y RESULTADO MÍNIMO	No aplica		
PRESENTACIÓN Y CONDICIONES DE LA MUESTRA.	No aplica		
REQUIERE ANTICIPO	No	PORCENTAJE DE ANTICIPO: No aplica	
ORIGEN DE LOS BIENES	No aplica		
NORMAS QUE APLICAN	No aplica		
LARLAS MÉTODO DE EVALUACIÓN (sólo aplica en Licitación o Invitación)	PUNTOS Y PORCENTAJES	COSTO BENEFICIO	BINARIO **X**
MODALIDAD DE	ABIERTO [ ]	CERRADO [X]	

CONTRATO	
ES UNA CONTRATACIÓN PLURIANUAL	**SI** [ ] **NO** [X]
VIGENCIA DEL CONTRATO.	**Vigencia del Contrato:** del día hábil siguiente a la notificación del fallo y hasta el 31 de diciembre de 2024. **Vigencia del servicio:** dentro de los 45 días posteriores a la notificación del fallo y hasta el 31 de diciembre de 2024.
LUGAR Y CONDICIONES DE LA ENTREGA DE LOS SERVICIOS.	Reiscom, S.A. de C.V. deberá entregar los equipos en los sitios indicados en el Anexo A.
MECANISMOS DE COMPROBACIÓN, SUPERVISIÓN Y VERIFICACIÓN DE LO ESTABLECIDO EN CONTRATOS	Se efectuará a través de la revisión de los entregables que se indican en el punto 11 del anexo técnico.
ENTREGABLES	Se indican en el punto 11 del anexo técnico.
FORMA Y PLAZO DE PAGO	Se indican en el punto 17 del anexo técnico.
NOMBRE Y CARGO DEL ADMINISTRADOR Y DEL SUPERVISOR DEL INSTRUMENTO JURÍDICO	Titular del Área Requirente y Administrador del Contrato. María Dolores Durán Márquez Subdirectora de Recursos Tecnológicos Supervisor del Contrato Roberto Ramírez Guzmán Jefe del Departamento de Soporte Técnico, Centro de Datos y Comunicaciones
FORMA Y TÉRMINOS EN QUE SE REALIZARÁ LA VERIFICACIÓN DE LAS ESPECIFICACIONES Y LA ACEPTACIÓN DE LOS BIENES	La aceptación de los servicios se notificará mediante oficio de liberación para el pago de servicios a mes calendario, previa aceptación del informe mensual firmado de manera autógrafa por el Responsable de Informática de la Unidad de Operación y por los Direcciones o Subdirectores de Área de Oficinas Centrales que contenga el resumen de los servicios realizados

1. Descripción de los equipos

El Instituto Nacional para la Educación de los Adultos (INEA) requiere de:

- El arrendamiento de equipo para telefonía IP.

Los equipos para telefonía IP se deberán suministrar de acuerdo con lo especificado en las características técnicas e incluir como mínimo los elementos de hardware, software, licenciamiento y funcionalidades requeridas en el presente anexo técnico. Reiscom, S.A. de C.V. deberá considerar en su propuesta que el INEA ya cuenta con un conmutador marca Alcatel Lucent, modelo OXO Compact Edition release 6.0/121.001 en las Unidades de Operación Ciudad de México, Estado de México, Michoacán y Nuevo León; con un conmutador marca Panasonic modelo KX-TDA100D reléase PBX Unified V7.8.1.1 en la Unidad de Operación Baja California y con un conmutador marca Unify openscape voice V9R1.22.5 en Oficinas Centrales por lo cual los equipos que oferte deberá garantizar su compatibilidad y correcto funcionamiento con dichos conmutadores.

La finalidad de la contratación es proporcionar a las áreas que la integran las herramientas tecnológicas en materia de telefonía IP, que permitan la interconexión para los servicios de Voz, Datos y video, bajo el protocolo IP, a fin de mantener la continuidad de los servicios que proporciona y, de esta manera, alcanzar sus metas.

Cuadro 1. Equipos en arrendamiento requeridos para telefonía IP

Partida	Tipo	Componente	Unidad de medida
1	Equipo telefonía IP	Terminal IP Básica	Equipo
2		Terminal IP Ejecutiva	Equipo
3		Servicio de tarificación telefónica (No. de extensiones a tarificar)	Equipo o licencia

2. Método de evaluación

El método de evaluación de las propuestas será binario.

3. Forma de adjudicación

En caso del arrendamiento del equipo de una sola partida esta será adjudicada por partida completa a un solo Proveedor.

En el caso de que se requieran en arrendamiento dos o más de los equipos agrupados por el tipo de telefonía IP definidos en las partidas del cuadro que antecede, estos tendrán que ser propuestos y adjudicados a un mismo Proveedor que reúna en su conjunto las mejores condiciones en cuanto a precio.

4. Criterios aplicables para el arrendamiento de equipo para telefonía IP

Reiscom, S.A. de C.V. en su cotización deberá considerar lo siguiente:

- Que las especificaciones plasmadas en el presente anexo técnico son los requerimientos mínimos para la contratación.
- Todos los equipos suministrados, incluidos los de reemplazo, deberán ser nuevos.
- Deberá realizar la instalación, configuración y puesta a punto de los equipos propuestos en las instalaciones indicadas en el Anexo A, además de garantizar la integración y compatibilidad de los componentes de Hardware descritos en el presente anexo técnico, así como los elementos necesarios para la integración y funcionalidad total requerida por INEA.
- Deberá incluir en su propuesta todas las actualizaciones del Software necesario para el correcto funcionamiento de los equipos descritos en el presente anexo técnico durante la vigencia del servicio.
- En el caso de que se requieran en arrendamiento dos o más de los equipos agrupados por el tipo de telefonía IP definidos en las partidas del cuadro que antecede, estos tendrán que ser propuestos y adjudicados a un mismo Proveedor que reúna en su conjunto las mejores condiciones en cuanto a precio.
- Reiscom, S.A. de C.V. deberá entregar dentro de los primeros quince días hábiles posteriores a la fecha de notificación del fallo un plan de trabajo donde se describan las actividades que se tienen que realizar para la correcta entrega, instalación, configuración y puesta a punto de los equipos requeridos por el INEA con aprobación de la misma.
- Reiscom, S.A. de C.V. como proveedor de los equipos para telefonía IP deberá incluir en su propuesta, el suministro de todos los accesorios necesarios, licenciamiento, actualizaciones de firmware por 12 meses y software para la correcta instalación, integración, operación y funcionalidad de los equipos con el conmutador marca Alcatel Lucent, modelo OXO Compact Edition release 6.0/121.001 en las Unidades de Operación Ciudad de México, Estado de México, Michoacán y Nuevo León; con un conmutador marca Panasonic modelo KX-TDA100D reléase PBX Unified V7.8.1.1 en la Unidad de Operación Baja California y con un conmutador marca Unify openscape voice V9R1.22.5 en Oficinas Centrales
- El tiempo de entrega, instalación, configuración y puesta a punto de los equipos propuestos en las instalaciones indicadas en el Anexo A, se deberá realizar dentro de un plazo no mayor a 45 días a partir de la fecha de notificación del fallo.
- Deberá realizar la entrega de los equipos para telefonía IP requeridos por el INEA en los domicilios indicados en el Anexo A
- El tiempo de atención vía telefónica será en un tiempo no mayor a 15 minutos, y se brindará durante 24 horas, los 7 días a la semana, los 365 días del año; cuando sea necesaria la atención en sitio esta deberá otorgarse dentro de las 24 horas naturales siguientes al levantamiento del reporte; cuando la resolución del reporte implique reemplazo de partes, el tiempo de solución máximo será de 48 horas naturales para la Ciudad de México, Área Metropolitana y para las zonas foráneas a partir del levantamiento del reporte.
- Reiscom, S.A. de C.V. deberá contar con medios de comunicación para reportar fallas de equipo (mesa de ayuda). Los medios para reportar fallas, al menos deberán ser un número convencional, un celular y un correo electrónico.
- Reiscom, S.A. de C.V. será responsable en el caso de que se violen derechos de propiedad industrial, patentes o derechos de autor, respecto al software y/o hardware utilizados en los equipos, dejando en todo momento a salvo al INEA.
- Reiscom, S.A. de C.V. proveerá los recursos humanos necesarios para cumplir las tareas de:
    - Maniobra, carga, descarga, desembalaje, ensamblado, retiro de empaques y entrega de los equipos.
    - Instalación, configuración y puesta a punto de los equipos, de acuerdo a las recomendaciones y mejores prácticas del fabricante.
- Reiscom, S.A. de C.V. será responsable de que la totalidad de componentes que conformen los equipos sean

compatibles.

5. Características técnicas de los equipos para telefonía IP

Reiscom, S.A. de C.V. deberá considerar en su propuesta técnica, todos los dispositivos telefónicos IP requeridos, los cuales deberán cumplir con las características técnicas y funcionalidades siguientes:

1.1.1.1. **5.1 TERMINAL IP BÁSICA**

- Deberá contar con una pantalla a color o monocromática de 2" o superior.
- Deberá contar por lo menos 2 líneas de apariencia.
- Deberá contar con botones programables y botones de funciones fijas (con LED) como altavoz, silencio y navegación.
- Deberá manejar historial de llamadas.
- Deberá contar con 2 puertos GE (10/100/1000).
- Deberá contar con POE.
- Deberá poder ser energizado a través de fuentes de alimentación e incluir la misma en caso de ser solicitada por el INEA.
- Deberá soportar los siguientes codecs de voz G.711A/μ, G.729ab, G.722, G.722.1, G.722.2, iLBC, Opus y AAC-LD
- Deberá manejar el almacenaje de múltiples contactos.
- Deberá manejar administración y mantenimiento remoto.
- Deberá manejar actualizaciones y aplicaciones de software automáticamente, así como administración vía web.
- Deberá manejar TLS/SRTP (AES 128).
- Deberá manejar 802.1P/Q, DSCP.
- Deberá contar con el licenciamiento para protocolo SIP estándar y/o IP que sea 100% compatible con el conmutador marca Alcatel Lucent, modelo OXO Compact Edition release 6.0/121.001 en las Unidades de Operación Ciudad de México, Estado de México, Michoacán y Nuevo León; con un conmutador marca Panasonic modelo KX-TDA100D reléase PBX Unified V7.8.1.1 en la Unidad de Operación Baja California y con un conmutador marca Unify openscape voice V9R1.22.5 en Oficinas Centrales. Deberá incluir las actualizaciones de firmware por 12 meses, tanto de la terminal como del conmutador a donde se conecte la terminal

1.1.1.2.

1.1.1.3. **5.2 TERMINAL IP EJECUTIVA**

- Deberá contar con una pantalla táctil de por lo menos 7" y 1280x800 píxeles.
- Deberá soportar como característica, un sistema operativo a través del cual sea posible instalar y desinstalar aplicaciones y que cuente con soporte de comunicación para voz y video.
- Deberá contar con POE.
- Deberá poder ser energizado a través de fuente de alimentación e incluir la misma en caso de ser solicitada.
- Deberá soportar los siguientes codecs de voz G.711A/μ, G.729ab, G.722, iLBC y opus.
- Deberá manejar administración y mantenimiento vía remota.
- Deberá soportar micrófono embebido con cámara.
- Deberá manejar TLS/SRTP (AES 128).
- Deberá soportar video conferencia.
- Deberá contar con el licenciamiento para protocolo SIP estándar y/o IP que sea 100% compatible con el conmutador marca Alcatel Lucent, modelo OXO Compact Edition release 6.0/121.001 en las Unidades de Operación Ciudad de México, Estado de México, Michoacán y Nuevo León; con un conmutador marca Panasonic modelo KX-TDA100D reléase PBX Unified V7.8.1.1 en la Unidad de Operación Baja California y con un conmutador marca Unify openscape voice V9R1.22.5 en Oficinas Centrales. Deberá incluir las actualizaciones de firmware por 12 meses, tanto de la terminal como del conmutador a donde se conecte la terminal

1.1.1.4. **5.3 MECANISMOS DE CIFRADO PARA VOZ**

Para asegurar la confidencialidad e integridad de la información de voz, así como del modelo propuesto para la solución de Telefonía IP, Reiscom, S.A. de C.V. deberá considerar en su propuesta técnica, que el Sistema de Procesamiento de Llamadas IP, que el hardware, software y licenciamiento necesarios que se utilicen para proporcionar el servicio de Voz IP y funcionalidades solicitadas, deberán contar con los elementos necesarios para garantizar, el cumplimiento de los siguientes mecanismos de seguridad, Reiscom, S.A. de C.V. deberá considerar en su propuesta que el INEA ya cuenta con un conmutador marca Alcatel Lucent, modelo OXO Compact Edition release 6.0/121.001 en las Unidades de Operación Ciudad de México, Estado de México, Michoacán y Nuevo León; con un conmutador marca Panasonic modelo KX-TDA100D reléase PBX Unified V7.8.1.1 en la Unidad de Operación Baja California y con un conmutador marca Unify openscape voice V9R1.22.5 en Oficinas Centrales por lo cual los equipos que oferte deberá garantizar su compatibilidad y correcto funcionamiento con dichos conmutadores..

- La solución propuesta deberá garantizar la encriptación de la llamada de punto a punto y en conferencia al menos AES-256 y los protocolos SRTP (Secure Real-time Transport Protocol) y TLS (Transport Layer Security), definidos en los RFC 3711 y RFC 2246 respectivamente. Esta condición aplicará solamente entre teléfonos IP y equipos y dispositivos que formen parte de la solución de Telefonía IP del INEA y para las llamadas establecidas entre ellas.
- Los teléfonos IP y las extensiones configuradas a través de software, deberán manejar mecanismos de encriptación basados en al menos en AES-256, con la utilización del protocolo SRTP para el transporte de la voz y por medio de al menos en AES- 128 y TLS para la señalización de la misma llamada.
- La solución deberá garantizar que la modalidad de encriptación solicitada anteriormente se mantendrá en comunicaciones establecidas con el correo de voz desde la red instalada en el INEA.
- El modelo de encriptación solicitado se deberá mantener con cualquier Gateway de Voz IP que esté en operación en la solución de Comunicaciones IP propuesta por Reiscom, S.A. de C.V., bajo los estándares solicitados.
- Reiscom, S.A. de C.V. deberá garantizar en su propuesta, que durante la vigencia del Contrato la infraestructura para proporcionar el servicio de Voz IP puede operar en su conjunto con una técnica de encriptación superior a AES-128, que será implementada sin ningún costo adicional para el INEA. Reiscom, S.A. de C.V. deberá realizar una evaluación previa, para determinar el impacto del cambio, de los cuales deberá informar al INEA para la toma de decisiones conjuntas.
- El Sistema de Procesamiento de Llamadas IP propuesto, deberá contar con la capacidad de manejar Códigos de Seguridad personales de 5 dígitos como mínimo, para hacer uso de facilidades telefónicas como llamada a celular y/o larga distancia, en cualquier teléfono físico basado en hardware de la Red.
- El modelo de Comunicaciones IP propuesto, deberá incluir mecanismos de autenticación a nivel digital, que permitan a los teléfonos IP autenticarse con el Sistema de Procesamiento de Llamadas IP, por medio de certificados digitales para garantizar que son dispositivos válidos en la Red con la categoría establecida.
- El Sistema de Procesamiento de Llamadas IP, así como los Gateway de voz propuestos en la solución, deben incluir y soportar, mecanismos internos de seguridad como; accesos a administración vía HTTPS (Hyper Text Transfer Protocol Secure) y/o CLI por medio de TELNET y SSH.

1.1.1.5. **5.4 SERVICIO DE TARIFICACIÓN TELEFÓNICA**

Para la operación de tarificación se requiere un sistema de procesamiento del registro detallado de llamadas, CDR (Call Detail Recording por sus siglas en inglés), esta facilidad proporciona el detalle de las operaciones que realiza el sistema de telefonía.

- Número de llamadas por categorías:
  - Móvil
  - Fijo
  - Local
  - Nacional
  - Internacional
- Fecha, hora y duración de llamadas.
- Origen y destino.
- Costos de llamada por Proveedor y tipo de llamada.
- Identificar códigos de autorización por usuario.

Los resultados generados por el reporte avanzado deberán ser impresos, exportados en diferentes formatos o visualizados en pantalla.

Obtención de reportes de Directorio Telefónico de extensiones, ordenar por número de extensión, alfabético por nombre o por departamento.

Reiscom, S.A. de C.V. deberá considerar en su propuesta que el INEA ya cuenta con un conmutador marca Alcatel Lucent, modelo OXO Compact Edition release 6.0/121.001 en las Unidades de Operación Ciudad de México, Estado de México, Michoacán de Ocampo y Nuevo León; con un conmutador marca Panasonic modelo KX-TDA100D reléase PBX Unified V7.8.1.1 en la Unidad de Operación Baja California y con un conmutador marca Unify openscape voice V9R1.22.5 en Oficinas Centrales, por lo cual los equipos y solución que oferte deberá garantizar su compatibilidad y correcto funcionamiento con dichos conmutadores.

1.1.1.6. **5.5 CORREO DE VOZ CON SERVICIOS DE MENSAJERÍA**

Reiscom, S.A. de C.V. deberá considerar en su propuesta técnica como parte de la solución para los Servicios de Voz, los

Sistemas de Correo de Voz con Servicios de Mensajería, mismos que el Administrador del Contrato del INEA, validará y/o ajustará en la fase de planeación para efectos de la implementación, sin embargo, durante la vigencia del contrato podrán ser modificados en cantidades de acuerdo con las solicitudes del INEA, sin costo de implementación adicional para el INEA lo anterior para ofrecer estas funcionalidades a los usuarios del Servicio integral de telefonía y telecomunicaciones, sin importar el sitio donde se encuentren.

La solución de Correo de Voz con Servicios de Mensajería para el Servicio de telefonía IP, deberán cumplir con las características técnicas y/o funcionalidades siguientes:

- Contar con la capacidad de habilitar el servicio de mensajería de voz por usuario, el cual podrá ser consultado mediante una tecla de acceso rápido en el teléfono, con el uso de una clave de usuario y contraseña como medida de seguridad.
- Contar con la facilidad de acceso a los mensajes de voz, desde cualquier teléfono dentro o fuera de la Red del INEA, marcando a un número directo donde deberá contestar una grabación que solicite el número de extensión y contraseña del buzón de voz y, en caso de ser válidos, indicará la cantidad de mensajes que se tienen pendientes de escuchar, permitiendo escuchar los, guardar los o borrarlos.
- Contar con la capacidad de personalizar un mínimo de 3 diferentes mensajes de bienvenida, configurables por el administrador del Sistema o por el usuario a través de su Teléfono IP, que se puedan activar o desactivar a consideración del usuario o administrador del sistema (opcional).
- Contar con la funcionalidad de aviso de mensajes de voz normal y/o urgente.
- Contar con la funcionalidad de poder asociar extensiones alternas configurables por el administrador o por el usuario, asociadas a un mismo buzón de voz.
- El Servicio de correo de voz deberá soportar SMTP para enviar los mensajes de voz vía correo electrónico a los usuarios. La solución deberá permitir que, al abrir el mensaje, este pueda ser escuchado y manejado por medio de controles que permitan avanzar, retroceder, detener, acelerar o ralentizar el mensaje para su mejor comprensión.
- La solución de Mensajería deberá contar con capacidad de almacenaje para cada uno de los buzones de mensajes de voz de al menos 5 minutos y soportar protocolos SIP y SRTP. La cantidad de canales hacia la solución de correo de voz con mensajería requerida será determinada por el INEA, así como la cantidad de mensajes por buzón a almacenar.

Reiscom, S.A. de C.V. deberá considerar en su propuesta que el INEA ya cuenta con un conmutador marca Alcatel Lucent, modelo OXO Compact Edition release 6.0/121.001 en las Unidades de Operación Ciudad de México, Estado de México, Michoacán y Nuevo León; con un conmutador marca Panasonic modelo KX-TDA100D reléase PBX Unified V7.8.1.1 en la Unidad de Operación Baja California y con un conmutador marca Unify openscape voice V9R1.22.5 en Oficinas Centrales, por lo cual los equipos y solución que oferte deberá garantizar su compatibilidad y correcto funcionamiento con dichos conmutadores.

1.1.2.

1.1.2.1. **5.12 SERVICIO DE OPERADORA AUTOMÁTICA**

Se entenderá Como Servicios de Operadora Automática, funcionalidad asociada a un Sistema de Procesamiento de Llamadas IP, para que las llamadas de usuarios externos o internos, dirigidas a un número de grupo de troncales del INEA, las distribuya el sistema de procesamiento a la operadora automática, misma que le ofrecerá al usuario de forma automática la opción de consulta y/o solicitud de información o enviarlo a una determinada extensión (con o sin DID asociado).

Por lo anterior Reiscom, S.A. de C.V. deberá considerar en su propuesta técnica el Servicio de Operadora Automática cumpliendo con lo siguiente:

- El Servicio de Operadora Automática deberá proveer un menú de opciones de navegación, para dividir fácilmente el tráfico en áreas de atención y, en caso de solicitarlo el INEA, en requerimientos de información más especializados, para canalizar las llamadas a su destino correspondiente. El administrador del contrato del INEA, en conjunto con Reiscom, S.A. de C.V. en caso que resulte adjudicado, establecerán en la fase de planeación los menús de navegación y la política para el desborde de las llamadas, así mismo, la solución deberá contar con la posibilidad de ofrecer dos menús, uno para el día (horario hábil de atención), y uno para la noche (informativo), de acuerdo a las solicitudes del INEA.
- Cuando se seleccione una opción inválida en el menú, se deberá transferir la llamada al inicio del mismo. Si no se selecciona ninguna opción del menú, la llamada deberá transferirse automáticamente al Servicio de Operadora Manual después de un tiempo programable.
- La Operadora Automática deberá contar con la facilidad de enrutar la llamada hacia algún número de extensión del INEA con o sin DID asociado, siempre y cuando la persona que llama lo conozca y lo digite. El Sistema de Procesamiento de Llamadas IP, deberá poder supervisar la transferencia de la llamada, si el usuario se encuentra en estado libre o desviado a otra extensión, la llamada se transferirá, si el usuario está ocupado, la persona que llama será dirigida al buzón de voz del mismo, en caso de contar con este servicio.
- El Servicio de Operadora Automática deberá operar de forma centralizada en los sitios donde lo solicite el INEA,

atendiendo cada uno, las llamadas entrantes de los números de grupo de las troncales del sitio asociado.

- Cada solución de Operadora Automática que solicite el INEA, deberá manejar los puertos de acceso definidos por el INEA, para las peticiones y/o consultas que realicen los usuarios externos e internos.
- La solución de Operadora Automática, deberá contar con la capacidad de manejar una determinada cantidad de sesiones concurrentes hacia cada uno de los sitios de la Red del INEA, conforme a los requerimientos de éstas y con base a la capacidad de puertos solicitados para cada Operadora Automática. En su caso, la asignación de sesiones concurrentes se determinará de común acuerdo entre el administrador del contrato del INEA y Reiscom, S.A. de C.V. en caso de que resulte adjudicado.
- El Sistema de Procesamiento de Llamadas IP deberá contar con la capacidad de desbordar a las Operadoras Automáticas, las llamadas externas que ingresen por los Números de Grupo de las troncales de los sitios, donde se cuente con este tipo de servicios, conforme a los requerimientos que establezca el administrador del contrato del INEA.

Reiscom, S.A. de C.V. deberá considerar en su propuesta que el INEA ya cuenta con un conmutador marca Alcatel Lucent, modelo OXO Compact Edition release 6.0/121.001 en las Unidades de Operación Ciudad de México, Estado de México, Michoacán y Nuevo León, y con un conmutador marca Panasonic modelo KX-TDA100D reléase PBX Unified V7.8.1.1 en la Unidad de Operación Baja California y con un conmutador marca Unify openscape voice V9R1.22.5 en Oficinas Centrales, por lo cual los equipos y solución que oferte deberá garantizar su compatibilidad y correcto funcionamiento con dichos conmutadores.

6. Manuales para equipos de telefonía IP

Se deberá de entregar manual del equipo para su instalación, configuración y operación impreso, en medio electrónico y en idioma español, además deberá proporcionar la liga del sitio web en el cual se puede descargar.

7. Medios para reportar fallas para equipos de Telefonía IP

- Reiscom, S.A. de C.V. deberá entregar el procedimiento de recepción de reportes y atención de fallas de los equipos, dentro de los 5 días hábiles posteriores a la fecha de notificación del fallo.
- Se deberá indicar una línea telefónica del fabricante o centro de atención telefónica certificado o aprobado por el fabricante sin costo de llamada para el usuario y un correo electrónico del fabricante, como canales para hacer efectiva la garantía de los equipos.

8. Requerimientos para equipos de telefonía IP

Los equipos ofertados por Reiscom, S.A. de C.V., por partida deberán ser nuevos de una misma marca y modelo y deberán cumplir con las características técnicas, solicitadas en el presente anexo técnico.

Reiscom, S.A. de C.V. deberá presentar como parte de su propuesta técnica la siguiente documentación:

- Carta original, en papel membretado y vigente, firmada por el fabricante de los equipos a ofertar detallando marca y modelo de los equipos propuestos y que certifique la configuración de los equipos propuestos para cada una de las partidas descritas en el presente anexo técnico.
- Carta original, en papel membretado y vigente, firmada por el fabricante de los equipos a ofertar en donde designe al Proveedor como distribuidor autorizado y certificado de los equipos propuestos.
- Carta original, en papel membretado y vigente, firmada por el fabricante de los equipos a ofertar en donde manifieste que Reiscom, S.A. de C.V. cuenta con personal certificado por el fabricante para la instalación, configuración y puesta a punto de los equipos propuestos.
- Carta original, en papel membretado y firmada por el fabricante en la que se relacionen sus centros de servicio autorizados.
- Carta original del fabricante en la que se manifieste que cuentan con la infraestructura técnica y de servicio y que garantiza la existencia de refacciones para el mantenimiento de los bienes objeto del arrendamiento, durante la vigencia del contrato de arrendamiento.
- Carta original del fabricante en la que se manifieste que los equipos objeto del arrendamiento, no tendrán un anuncio de fin de vida ni anuncio de fin de mantenimiento durante la vigencia del contrato de arrendamiento.
- Reiscom, S.A. de C.V. deberá presentar dentro de su propuesta técnica, los documentos impresos con los que se acredite el cumplimiento de las normas y certificaciones requeridas en el presente anexo técnico, en la ficha técnica deberá identificar cada una de las características técnicas solicitadas para los equipos descritos en las diferentes partidas. Los catálogos o folletos deberán estar impresos en idioma español; de no ser así, se deberá acompañar a estos con una traducción al español. En caso que alguna referencia solicitada no se refleje en la ficha técnica del equipo, pero si este soportado por el fabricante, el INEA aceptará una carta de fabricante mencionando el soporte de la funcionalidad solicitada.

- Carta original, en papel membretado y firmada por Reiscom, S.A. de C.V. en el que manifieste que los equipos que ofertará y suministrará son nuevos, no armados, no re-manufacturados y de modelos recientes (máximo dos años), especificando la fecha de inicio de comercialización del equipo.

9. Capacitación

- Reiscom, S.A. de C.V. deberá incluir en su propuesta curso de capacitación del equipo para Red telefonía IP impartido en un centro de capacitación autorizado y avalado por el fabricante, para al menos dos personas, con una duración mínima de 40 horas.
- Los cursos de capacitación deberán incluir la operación, administración y configuración de los bienes propuestos.
- La fecha en que se realizará la capacitación será definida entre Reiscom, S.A. de C.V. y el INEA.

10. Instalación

La instalación, configuración y puesta a punto de los bienes ofertados deberá ser realizada por parte de Reiscom, S.A. de C.V. y de común acuerdo con el INEA.

- Para la instalación, configuración y puesta a punto de los bienes ofertados, Reiscom, S.A. de C.V. deberá entregar un plan de trabajo al Administrador del Contrato del INEA quien aprobará dicho plan.
- El INEA determinará la ubicación física en donde se requiera instalar los equipos los cuales se indican en el Anexo A.

11. Entregables para equipos de telefonía IP

Los entregables se definen como la entrega de los equipos, documentación inicial, final y reportes mensuales inherentes al presente Anexo Técnico, es responsabilidad de Reiscom, S.A. de C.V. entregarlos al Administrador del Contrato del INEA.

El Administrador del Contrato del INEA y el representante designado por Reiscom, S.A. de C.V. serán responsables de dar seguimiento y cumplimiento a lo establecido en el presente anexo técnico.

Reiscom, S.A. de C.V. deberá entregar de forma electrónica, archivos con la relación en la que se indique marca, modelo y número de serie.

Se hará constar la entrega del equipo con el usuario final, a través del formato de resguardo de telefonía IP, el equipo deberá entregarse con el número de extensión asignada. El usuario que recibe el equipo validará su correcto funcionamiento, por lo que Reiscom, S.A. de C.V. deberá obtener la firma de conformidad del usuario en el formato de resguardo, el machote de formato de resguardo será proporcionado al proveedor por la Subdirección de Recursos Tecnológicos del INEA, dichos formatos de resguardos deberán ser administrados por personal dReiscom, S.A. de C.V. y proporcionar una copia al Administrador del Contrato.

Dentro de los primeros quince (15) días hábiles posteriores a la notificación del fallo, Reiscom, S.A. de C.V. deberá entregar lo siguiente:

- Cronograma de actividades.
- El plan de trabajo detallado para la instalación, configuración y puesta a punto de los bienes ofertados para el INEA, con aprobación de las mismas. El plan de trabajo deberá incluir la definición, desarrollo y mantenimiento de un plan de pruebas para validar la correcta instalación, configuración y puesta a punto.
- Reiscom, S.A. de C.V. deberá entregar una matriz de escalamiento que permita al INEA contactar al personal designado por Reiscom, S.A. de C.V. para asegurar el cumplimiento conforme al presente anexo técnico. De igual manera, Reiscom, S.A. de C.V. deberá proporcionar un documento donde se plasme el procedimiento que seguirá para resolución de incidentes
- Reiscom, S.A. de C.V. deberá entregar el procedimiento de recepción de reportes para la atención y resolución de fallas de los equipos dentro de los cinco (5) días hábiles posteriores a la fecha de notificación del fallo.

Memoria técnica dentro de los primeros diez (10) días hábiles posteriores a la puesta en operación de los equipos de telefonía IP conteniendo lo siguiente:

- Relación de equipos utilizados para la implementación de la solución.
- Diagramas de conectividad. Los diagramas se incluirán dentro de la memoria técnica en formato electrónico (Microsoft Office Visio).
- Registro de las pruebas de conectividad realizadas.
- Reiscom, S.A. de C.V. deberá incluir una copia del respaldo de los equipos de la solución implementada en medio magnético.
- En caso de sustitución de equipos o cambio de configuración en los mismos, la memoria técnica deberá ser actualizada por Reiscom, S.A. de C.V..

Entregables mensuales

- Entrega dentro de los primeros 10 días hábiles siguientes a la conclusión del mes que se pretende facturar, de los siguientes documentos:
    - Informe mensual firmado de manera autógrafa por el Responsable de Informática de la Unidad de Operación y por los Directores de Área de Oficinas Centrales que contenga el resumen de los servicios realizados, el original deberá entregarse a la Subdirección de Recursos Tecnológicos, el informe debe adjuntar:
        - Reportes de los servicios correctivos presentados, solucionados y aquellos que no hayan cumplido con los SLA´s definidos durante el mes,
        - Informe mensual que contenga las métricas de cumplimiento de los niveles de servicio.
        - Reporte de trazabilidad que contiene el detalle de los equipos que fueron reparados y asignados a otras áreas durante el mes analizado.
        - Reporte de reemplazo por seguro que contiene el detalle de los equipos que fueron tramitados y atendidos por el seguro de Reiscom, S.A. de C.V., donde se indica la fecha en que se levantó, y la fecha de entrega al usuario.
        - Reporte de acumulado de equipos atendidos por garantía y devolución de préstamo. Contiene los reportes generados durante el mes analizado y aquellos reportes no cerrados en el mes inmediato anterior, a los cuales se les proporciono un equipo en préstamo en tanto se realiza el trámite de garantía correspondiente. El reporte incluye entre otros datos, folio de servicio, número de ticket, fecha de hora de inicio y cierre lo anterior a fin de realizar los cálculos de los niveles de servicios considerados en el presente anexo técnico
    - Relación total de los equipos entregados en arrendamiento por parte de Reiscom, S.A. de C.V. a entera satisfacción del INEA.
    - Reporte de incidencias.

12. Mesa de ayuda para equipos de telefonía IP

Reiscom, S.A. de C.V. deberá poner a disposición del INEA una mesa de ayuda dentro de los 5 días hábiles posteriores contados a partir de la primera entrega de equipo para que el INEA puedan reportar las fallas de los equipos de Telefonía IP, para lo cual Reiscom, S.A. de C.V. deberá proporcionar números convencionales y celulares, además de correos electrónicos del representante designado por Reiscom, S.A. de C.V..

13. Niveles de atención para equipos de telefonía IP

Los tiempos de atención y solución de fallas requeridos son:

- La garantía en sitio de los bienes. Se cubrirá en las instalaciones indicadas en el Anexo A en la que se encuentre instalado el equipo.
- El tiempo de atención vía telefónica será en un tiempo no mayor a 15 minutos, y se brindará durante 24 horas, los 7 días a la semana, los 365 días del año; cuando sea necesaria la atención en sitio, ésta deberá otorgarse dentro de las 24 horas naturales siguientes al levantamiento del reporte; cuando la resolución del reporte implique reemplazo de partes, el tiempo de solución máximo será de 48 horas naturales para la Ciudad de México, Área Metropolitana y para las zonas foráneas, a partir del levantamiento del reporte
- Si el tiempo de reparación excede el tiempo establecido en los puntos antes mencionados, al día siguiente hábil, Reiscom, S.A. de C.V. deberá entregar un equipo de respaldo equivalente mientras se soluciona el problema.
- Si el equipo presenta más de cinco fallas dentro de un periodo de 30 días naturales, Reiscom, S.A. de C.V. deberá sustituirlo por uno de características iguales o superiores, en un plazo no mayor a un día hábil a partir del quinto reporte de falla en el mes para la Ciudad de México y Área Metropolitana y dos días hábiles a partir del quinto reporte de falla en el mes para las zonas foráneas incluyendo el tiempo de atención.
- Si la reparación excede los 30 días naturales a partir de la fecha del reporte, al día siguiente hábil, Reiscom, S.A. de C.V. entregará a cambio un equipo nuevo con las características iguales o superiores al arrendado.

En caso de reasignación o reubicación, se atenderá lo siguiente:

- Dicha solicitud deberá atenderse a partir del levantamiento del reporte por parte del Administrador del Contrato, en un plazo no mayor a dos (2) días hábiles cuando la reasignación o reubicación se realice dentro del mismo inmueble, y dentro del plazo de tres (3) días hábiles cuando la reasignación o reubicación de los equipos deba efectuarse en inmuebles diferentes del INEA, siempre que éstos se localicen en la Ciudad de México y Área

Metropolitana. Los plazos antes mencionados podrán ampliarse hasta por cinco (5) días hábiles cuando las reasignaciones o reubicaciones se realicen en las zonas foráneas. En todos los casos, se considerarán días laborables y en un horario de 9:00 a 19:00 horas. Dichos periodos incluirán el tiempo de atención.

Otros supuestos:

- En caso de robo o daño de los equipos destinados al arrendamiento por causas atribuibles al proveedor durante los procesos de entrega, o durante su instalación y/o configuración, Reiscom, S.A. de C.V. deberá sustituirlos por equipos con características iguales o superiores, dentro del plazo señalado en el numeral 15 “Plazo de entrega de los equipos”, sin otorgarse plazos adicionales para tal efecto y sin costo para el INEA.

Reiscom, S.A. de C.V. deberá proporcionar durante la vigencia de la garantía los niveles de atención descritos en la siguiente tabla:

Actividad	Descripción	Alcance	Nivel de servicio	
Entregables	Reiscom, S.A. de C.V. deberá entregar los equipos arrendados. Reiscom, S.A. de C.V. deberá entregar de forma electrónica, archivos con la relación en el que se indique marca, modelo y número de serie. Se hará constar la entrega del equipo con el usuario final, a través del formato de resguardo de telefonía IP, el equipo deberá entregarse con el número de extensión asignada. El usuario que recibe el equipo validará su correcto funcionamiento, por lo que Reiscom, S.A. de C.V. deberá obtener la firma de conformidad del usuario en el formato de resguardo, el machote de formato de resguardo será proporcionado al proveedor por la Subdirección de Recursos Tecnológicos del INEA, dichos formatos de resguardos deberán ser administrados por personal dReiscom, S.A. de C.V. y proporcionar una copia al Administrador del Contrato.	Arrendamiento de equipo para telefonía IP	Dentro de los 90 días naturales a partir de la notificación del fallo.	Aplicación de pena convencional del 5% sobre el monto mensual del pago previsto para los equipos no entregados, instalados, configurados y puestos en marcha, por cada día natural de atraso
Entregables	Reiscom, S.A. de C.V. deberá de entregar: El plan de trabajo detallado para la instalación, configuración y puesta a punto de los bienes ofertados con aprobación de las mismas. El plan de trabajo deberá incluir la definición, desarrollo y mantenimiento de un plan de pruebas para validar la correcta instalación, configuración y puesta a punto. Reiscom, S.A. de C.V. deberá entregar el procedimiento de recepción de reportes para la atención y resolución de fallas de los equipos dentro de los cinco (5) días hábiles posteriores a la notificación del fallo. Reiscom, S.A. de C.V. deberá entregar una matriz de	Arrendamiento de equipo para telefonía IP	Dentro de los primeros cinco (5) días hábiles posteriores a la notificación del fallo.	Aplicación de pena convencional, del 5% del valor del costo mensual del arrendamiento del equipo, por cada día natural de atraso

	escalamiento que permita al INEA contactar al personal designado por Reiscom, S.A. de C.V. para asegurar el cumplimiento conforme al presente anexo técnico. De igual manera, Reiscom, S.A. de C.V. deberá proporcionar un documento donde se plasme el procedimiento que seguirá para la resolución de incidentes.			
Entregables	Memoria técnica conteniendo: Relación de equipos utilizados para la implementación de la solución. Diagramas de conectividad. Los diagramas se incluirán dentro de la memoria técnica en formato electrónico (Microsoft Office Visio). Registro de las pruebas de conectividad realizadas. Reiscom, S.A. de C.V. deberá incluir una copia del respaldo de los equipos de la solución implementada en medio magnético. En caso de sustitución de equipos o cambios de configuración en los mismos, la memoria técnica deberá ser actualizada por Reiscom, S.A. de C.V..	Arrendamiento de equipo para telefonía IP	Dentro de los primeros diez (10) días hábiles posteriores a la puesta en operación de los equipos de telefonía IP.	Aplicación de pena convencional, del 5% del valor del costo mensual del arrendamiento del equipo, por cada día natural de atraso
Entregables mensuales	Reiscom, S.A. de C.V. deberá entregar dentro de los primeros 10 días hábiles siguientes a la conclusión del mes que se pretende facturar, los siguientes documentos: Informe mensual firmado de manera autógrafa por el Responsable de Informática de la Unidad de Operación y por los Directores o Subdirectores de Área de Oficinas Centrales que contenga el resumen de los servicios realizados El original deberá entregarse a la Subdirección de Recursos Tecnológicos, el informe debe adjuntar: Reportes de los servicios correctivos presentados, solucionados y aquellos que no hayan cumplido con los SLA´s definidos durante el mes, Informe mensual que contenga las métricas de cumplimiento de los niveles de servicio.	Arrendamiento de equipo para telefonía IP.	Dentro de los primeros diez (10) días hábiles siguientes a la conclusión del mes que se pretende facturar.	Aplicación de pena deductiva del 5% sobre el monto de la facturación del mes inmediato anterior por cada día natural de atraso

	Reporte de trazabilidad que contiene el detalle de los equipos que fueron reparados y asignados a otras áreas durante el mes analizado. Reporte de reemplazo por seguro que contiene el detalle de los equipos que fueron tramitados y atendidos por el seguro de Reiscom, S.A. de C.V., donde se indica la fecha en que se levantó, y la fecha de entrega al usuario. Reporte de acumulado de equipos atendidos por garantía y devolución de préstamo. Contiene los reportes generados durante el mes analizado y aquellos reportes no cerrados en el mes inmediato anterior, a los cuales se les proporciono un equipo en préstamo en tanto se realiza el trámite de garantía correspondiente. El reporte incluye entre otros datos, folio de servicio, número de ticket, fecha de hora de inicio y cierre lo anterior a fin de realizar los cálculos de los niveles de servicios considerados en el presente anexo técnico Relación total de equipos activos. Reporte de incidencias.			
Mesa de ayuda	Poner a disposición del INEA una mesa de ayuda para el levantamiento de reportes de fallas de los equipos	Arrendamiento de equipo para telefonía IP	Dentro de los cinco (5) días hábiles posteriores contados a partir de la primera entrega de equipo.	Aplicación de pena convencional, del 5% del valor del costo mensual del arrendamiento del equipo, por cada día natural de atraso por cada día natural de atraso
Atención de fallas	Atención y reparación de fallas y problemas relacionadas con los equipos	Arrendamiento de equipo para telefonía IP	El tiempo de atención vía telefónica será en un tiempo no mayor a 15 minutos, y se brindará durante 24 horas, los 7 días a la semana, los 365 días del año; cuando sea necesaria la atención en sitio, ésta deberá otorgarse dentro de las 24 horas naturales siguientes al levantamiento del reporte; cuando la resolución del reporte implique	Aplicación de pena deductiva del 5% sobre el monto de la facturación del mes inmediato anterior correspondiente al equipo que no sea sustituido, reparado o repuesto en los términos y plazos establecidos en el presente anexo por cada día natural de atraso

				reemplazo de partes, el tiempo de solución máximo será de 48 horas naturales para la Ciudad de México, Área Metropolitana y para las zonas foráneas, a partir del levantamiento del reporte. De implicarse la reparación de los equipos se atenderá lo siguiente: - Si el tiempo de reparación excede el tiempo establecido en los puntos antes mencionados, al día siguiente hábil, Reiscom, S.A. de C.V. deberá entregar un equipo de respaldo equivalente mientras se soluciona el problema. - Si la reparación excede los 30 días naturales a partir de la fecha del reporte, al día siguiente hábil, Reiscom, S.A. de C.V. entregará a cambio, instalar, configurar y poner a punto un equipo nuevo con las características iguales o superiores al arrendado - Si el equipo presenta más de cinco fallas dentro de un periodo de 30 días naturales, Reiscom, S.A. de C.V. deberá sustituirlo por uno de características iguales o superiores, en un plazo no mayor a un día hábil a partir del quinto reporte de falla en el mes para la Ciudad de México y Área	

			Metropolitana y dos días hábiles a partir del quinto reporte de falla en el mes para las zonas foráneas incluyendo el tiempo de atención.	
Reasignación o reubicación de los equipos otorgados en arrendamiento por Reiscom, S.A. de C.V. en la Ciudad de México, zona Metropolitana y zonas foráneas	Atención para la reasignación o reubicación de los equipos en las instalaciones o sedes del INEA.	Todos los equipos y servicios objeto del arrendamiento que se detallan en el presente Anexo Técnico e instalados en la Ciudad de México, zona Metropolitana y zonas foráneas.	En caso de reasignación o reubicación, se atenderá lo siguiente: Dicha solicitud deberá atenderse a partir del levantamiento del reporte por parte del Administrador del Contrato, en un plazo no mayor a dos (2) días hábiles cuando la reasignación o reubicación se realice dentro del mismo inmueble y en un plazo de tres (3) días hábiles cuando la reasignación o reubicación de los equipos deba efectuarse en inmuebles diferentes del INEA, siempre que éstos se localicen en la Ciudad de México y Área Metropolitana. Los plazos antes mencionados podrán ampliarse a cinco (5) días hábiles cuando las reasignaciones o reubicaciones se realicen en las zonas foráneas. En todos los casos se considerarán días laborables y en un horario de 9:00 a 19:00 horas. Dichos periodos incluirán el tiempo de atención	Aplicación de pena deductiva del 5% sobre el monto de la facturación del mes inmediato anterior correspondiente al equipo que no sea sustituido, reparado o repuesto en los términos y plazos establecidos en el presente anexo por cada día natural de atraso

14. Vigencia de la contratación

Vigencia del Contrato: del día hábil siguiente a la notificación del fallo y hasta el 31 de diciembre de 2024.
Vigencia del servicio: dentro de los 45 días posteriores a la notificación del fallo y hasta el 31 de diciembre de 2024.

15. Plazo de entrega de los equipos

La entrega de los equipos, su instalación, configuración y puesta a punto se deberá realizar en un plazo no mayor a 45 días naturales a partir del día hábil siguiente a la notificación del fallo.

Se hará constar la entrega del equipo con el usuario final, a través del formato de resguardo de telefonía IP, el equipo deberá entregarse con el número de extensión asignada. El usuario que recibe el equipo validará su correcto funcionamiento, por lo que Reiscom, S.A. de C.V. deberá obtener la firma de conformidad del usuario en el formato de resguardo, el machote de formato de resguardo será proporcionado al proveedor por la Subdirección de Recursos Tecnológicos del INEA, dichos formatos de resguardos deberán ser administrados por personal dReiscom, S.A. de C.V. y proporcionar una copia al Administrador del Contrato.

16. Lugar de entrega

Reiscom, S.A. de C.V. deberá entregar los equipos en los sitios indicados en el Anexo A.

17. Condiciones y forma de pago

El pago correspondiente se realizará dentro de los 20 días naturales contados a partir de la entrega de la factura, previa entrega, instalación, configuración y puesta a punto de los equipos a entera satisfacción del INEA en términos del presente Anexo técnico de conformidad con el artículo 51, de la LAASSP.

Lo anterior, quedará condicionado proporcionalmente al pago que Reiscom, S.A. de C.V. del equipo deba efectuar por concepto de penas convencionales o deducciones con motivo del incumplimiento en que pudiera incurrir.

Para el presente procedimiento queda especificado que el pago por el arrendamiento comenzará a correr a partir del siguiente día hábil de que el servicio quede debidamente configurado y en operación, a entera satisfacción del INEA.

18. Penas y deductivas

Penas convencionales

En el arrendamiento:

Reiscom, S.A. de C.V. se obliga a pagar al INEA una pena convencional del 5% sobre el monto mensual del pago previsto para los equipos no entregados, instalados, configurados y puestos en marcha, conforme a lo descrito en el numeral 15 del presente anexo técnico por cada día natural de atraso.

La misma pena se aplicará en el caso de no proporcionar la mesa de ayuda dentro de los 5 días hábiles posteriores contados a partir de la primera entrega de equipo.

En los entregables:

Reiscom, S.A. de C.V. se obliga a pagar al INEA una pena convencional por no presentar los entregables mensuales en los plazos establecidos en el numeral 11 del presente anexo técnico. Dicha pena será del 5% del valor del costo mensual del arrendamiento del equipo, por cada día natural de atraso.

Deductivas

Se aplicará una deductiva al Proveedor por el cumplimiento parcial o deficiente en el arrendamiento. Dicha deductiva será del 5%, sobre el monto de la facturación del mes inmediato anterior correspondiente al equipo que no sea sustituido o reparado en los términos y plazos establecidos en el presente anexo por cada día natural de atraso. Lo anterior, de conformidad en lo establecido en el artículo 53 bis de la LAASSP.

Igual porcentaje, se aplicará como deductiva en los casos que Reiscom, S.A. de C.V. suspenda el arrendamiento por cualquier causa injustificada, esto es fuera de los casos de fuerza mayor o caso fortuito debidamente acreditado y documentado en términos de la normatividad aplicable, por cada día natural que suspenda el arrendamiento, independientemente de que no se pagaría arrendamiento por el tiempo que dure la suspensión.

En caso de que los conceptos en los que subsistan el cumplimiento parcial o la deficiencia sean equivalentes al importe de la garantía otorgada por Reiscom, S.A. de C.V. del arrendamiento, el Administrador del Contrato podrá optar por cancelar total o parcialmente el arrendamiento aplicando la pena convencional máxima al Proveedor, lo anterior, en términos del artículo 100 del Reglamento de la Ley antes citada, o bien, optar por rescindir el contrato en término de la LAASSP.

19. Garantías

Garantía de cumplimiento

Para garantizar el cumplimiento del contrato que se le llegase adjudicar al Proveedor, se obliga a entregar dentro de los 10 (diez) días naturales siguientes a la fecha de firma del instrumento contractual, garantía (divisible o indivisible) en moneda nacional (pesos mexicanos) por el equivalente al 10% (diez por ciento) del importe del contrato que suscriba con el INEA, sin considerar el impuesto al valor agregado, la cual deberá emitir a favor de la Tesorería de la Federación o a quien en su caso corresponda y cumplir con los requisitos establecidos en el artículo 103 del reglamento de la LAASSP, aplicable en la materia.

La garantía se deberá de entregar en el domicilio del INEA.

20. Administrador del contrato

El Administrador del Contrato será el responsable de calcular y notificar al Proveedor, las penas convencionales y las deductivas que se hubieran determinado en el periodo de evaluación. Para la recepción del arrendamiento el Administrador del Contrato verificará el cumplimiento de las condiciones establecidas para el otorgamiento del arrendamiento, de conformidad con lo establecido en el penúltimo párrafo del artículo 84 del reglamento de la LAASSP.

21. Confidencialidad

Reiscom, S.A. de C.V. deberá presentar en su propuesta técnica carta en papel membretado firmada por el representante legal, donde se compromete a mantener absoluta confidencialidad de la información a la cual tengan acceso siendo responsable de cada uno de los integrantes del personal asignado para el desarrollo y operación del proyecto, respetando el manejo correcto. de la información.

Toda la información a que tenga acceso el personal que Reiscom, S.A. de C.V. designe para el cumplimiento del contrato, es considerada de carácter confidencial.

22. Responsabilidad laboral

El (Los) Proveedor (es) se constituye (n) como único patrón del personal que ocupe para llevar a cabo las acciones derivadas del presente procedimiento de contratación y será el único responsable de las obligaciones que en virtud de disposiciones legales y demás ordenamientos en materia de trabajo y seguridad Social, les deriven frente a dicho personal, liberando al INEA de cualquier responsabilidad laboral al respecto.

23. Cotización

Los Proveedores deberán cotizar por precios unitarios sin incluir el I.V.A. y en moneda nacional (pesos mexicanos), conforme al presente anexo técnico y a los formatos que se acompañan.

24. Transición del arrendamiento para la transmisión a título gratuito

Al concluir la vigencia del servicio, el prestador del servicio deberá transmitir la propiedad a título gratuito de la totalidad del equipamiento objeto de la contratación a favor del INEA.

Para que se lleve a cabo dicha transmisión de propiedad a título gratuito, el prestador del servicio queda obligado a entregar la factura correspondiente que contenga el inventario de los equipos, asimismo a firmar todos los documentos que se le requieran y resulten razonables para transferir a el INEA la propiedad de la totalidad del equipamiento objeto de la contratación, libres de todo gravamen y sin responsabilidades o contingencias; en el entendido de que el prestador del servicio deberá ceder al INEA todos los derechos que tenga el prestador del servicio con sus proveedores o con los fabricantes de los equipos, incluyendo las garantías que todavía se encuentren vigentes en la fecha de conclusión del servicio.

La transmisión de propiedad a título gratuito de la totalidad del equipamiento objeto de la contratación a favor del INEA deberá ser documentada en el contrato o convenio que al efecto se celebre, previa solicitud de la SRT en su calidad de supervisor y administrador del contrato a la SRMS.

¨LAS PARTES", deberán formalizar la donación de los equipos arrendados, con (30) treinta días hábiles previos a la terminación del contrato, en el entendido que no podrá realizarse el último pago pactado, si no se ha suscrito el contrato de donación respectivo.

Dicha falta no será imputable al "EL INEA" cuando se acredite que el retraso del pago pactado se atribuye a las omisiones de "REISCOM, S.A. DE C.V." o "PRESTADOR DEL SERVICIO".

25. Seguros

Seguro de equipos

Reiscom, S.A. de C.V. adjudicado se obliga en todo momento y situación a asumir la responsabilidad total por el

aseguramiento y gastos asociados que se generen con motivo de siniestro o robo de los bienes proporcionados para la prestación del arrendamiento, a continuación, se enuncian de manera ilustrativa mas no limitativa los siguientes casos:

- Robo de los equipos proporcionados para la prestación del arrendamiento.
- Incendio, impacto directo de rayo, implosión, explosión.
- Humo, hollín, gases, líquidos o polvos corrosivos, agua, humedad.
- Corto circuito, descargas eléctricas.
- Riesgo de transporte de los equipos (pérdida, robo o daño).
- Desgaste por el uso y manejo de los equipos derivado de la propia actividad.

Reiscom, S.A. de C.V. adjudicado se obliga a que en caso de siniestro o robo de los equipos en uso, los repondrá en un plazo no mayor a 5 días hábiles, sin costo adicional para el Instituto, en caso de no cumplir con este periodo se aplicará la pena convencional indicada en este Anexo Técnico.

Protesto lo necesario

Francisco Javier Murillo Pantoja
Representante Legal

Vanguardia Tecnológica Para Su Empresa

Instituto Nacional para la Educación de los Adultos
Invitación a cuando menos Tres Personas
Procedimiento No. IA-11-MDA-011MDA001-N-59-2024
Nombre del licitante: REISCOM, S.A. DE C.V.
Fecha: 29 de mayo de 2024

ANEXO 1
(Especificaciones Técnicas)

Nombre del Licitante: REISCOM, S.A. DE C.V.

Domicilio fiscal: ATLAPULCO 6A, COL. VERGEL DEL SUR, ALCALDÍA DE TLAPAN, CDMX

R.F.C.: REI0409133LA TELEFÓNO: 55 52643871

SERVICIO DE ARRENDAMIENTO DE EQUIPO PARA TELEFONÍA IP

PARTIDA	CARACTERÍSTICAS O TÉCNICAS DE LOS SERVICIOS	UNIDAD DE MEDIDA	CANTIDAD
1	**TERMINAL IP BÁSICA MARCA ALCATEL-LUCENT MODELO ALE-20** • Deberá contar con una pantalla monocromática de 2" Deberá contar por lo menos 2 líneas de apariencia. • Deberá contar con botones programables y botones de funciones fijas (con LED) como altavoz, silencio y navegación. • Deberá manejar historial de llamadas. • Deberá contar con 2 puertos GE (10/100/1000). • Deberá contar con POE. • Deberá poder ser energizado a través de fuentes de alimentación e incluir la misma en caso de ser solicitada por el INEA. • Deberá soportar los siguientes codecs de voz G.711A/μ, G.729ab, G.722, G.722.1, G.722.2, iLBC, Opus y AAC-LD • Deberá manejar el almacenaje de múltiples contactos. • Deberá manejar administración y mantenimiento remoto. • Deberá manejar actualizaciones y aplicaciones de software automáticamente, así como administración vía web. • Deberá manejar TLS/SRTP (AES 128). • Deberá manejar 802.1P/Q, DSCP. • Deberá contar con el licenciamiento para protocolo SIP estándar y/o IP que sea 100% compatible con el conmutador marca Alcatel Lucent, modelo OXO Compact Edition release 6.0/121.001 en las Unidades de Operación Ciudad de México, Estado de México, Michoacán y Nuevo León; Deberá incluir las actualizaciones de firmware por 12 meses, tanto de la	Servicio	01

	terminal como del conmutador a donde se conecte la terminal		
2	**TERMINAL IP EJECUTIVA MARCA ALCATEL-LUCENT MODELO ALE-300** • Deberá contar con una pantalla táctil de por lo menos 7" y 1280x800 píxeles. • Deberá soportar como característica, un sistema operativo a través del cual sea posible instalar y desinstalar aplicaciones y que cuente con soporte de comunicación para voz y video. • Deberá contar con POE. • Deberá poder ser energizado a través de fuente de alimentación e incluir la misma en caso de ser solicitada. • Deberá soportar los siguientes codecs de voz G.711A/µ, G.729ab, G.722, iLBC y opus. • Deberá manejar administración y mantenimiento vía remota. • Deberá soportar micrófono embebido con cámara. • Deberá manejar TLS/SRTP (AES 128). • Deberá soportar video conferencia. • Deberá contar con el licenciamiento para protocolo SIP estándar y/o IP que sea 100% compatible con el conmutador marca Alcatel Lucent, modelo OXO Compact Edition release 6.0/121.001 en las Unidades de Operación Ciudad de México, Estado de México, Michoacán y Nuevo León;	Servicio	01

3	**SERVICIO DE TARIFICACIÓN TELEFÓNICA**
	
	Para la operación de tarificación se requiere un sistema de procesamiento del registro detallado de llamadas, CDR (Call Detail Recording por sus siglas en inglés), esta facilidad proporciona el detalle de las operaciones que realiza el sistema de telefonía.
	
	• Número de llamadas por categorías:
	  ○ Móvil
	  ○ Fijo
	  ○ Local
	  ○ Nacional
	  ○ Internacional
	• Fecha, hora y duración de llamadas.
	• Origen y destino.
	• Costos de llamada por Proveedor y tipo de llamada.
	• Identificar códigos de autorización por usuario.
	
	Los resultados generados por el reporte avanzado deberán ser impresos, exportados en diferentes formatos o visualizados en pantalla.
	
	Obtención de reportes de Directorio Telefónico de extensiones, ordenar por número de extensión, alfabético por nombre o por departamento.
	
	El proveedor deberá considerar en su propuesta que el INEA ya cuenta con un conmutador marca Alcatel Lucent, modelo OXO Compact Edition release 6.0/121.001 en las Unidades de Operación Ciudad de México, Estado de México, Michoacán de Ocampo y
		Servicio	01

	Nuevo León;.		

NOTAS:

El Licitante REISCOM, describe lo solicitado, por el INEA en el ANEXO 1 (Especificaciones Técnicas y ANEXO A) en cuanto a partida, cantidad y unidad de medida.
En la columna de características técnicas de los servicios, transcribirá lo indicado en su propuesta técnica.

Protesto lo necesario

Francisco Javier Murillo Pantoja
Representante Legal

FOLIO. 22

Alcatel·Lucent Enterprise

CARTA CENTRO DE SERVICIOS

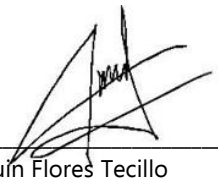
Instituto Nacional para la Educación de los Adultos
Invitación a cuando menos Tres Personas
Procedimiento No. IA-11-MDA-011MDA001-N-59-2024
Nombre del licitante: REISCOM, S.A. DE C.V.
Fecha: 29 de mayo de 2024

Por medio del presente y en el marco del proyecto de referencia, me dirijo a usted a efecto de informarle que la empresa Reiscom S.A. de C.V. cuenta con el siguiente centro de servicios autorizado.

Atlapulco No. 6A
Col. Vergel del Sur
Alcaldía de Tlalpan
C.P. 14340
Ciudad de México

Sin otro particular, quedo a sus órdenes.

Atentamente,



Joaquín Flores Tecillo
Channel Sales Leader
Alcatel Lucent Enterprise México
M. 5544993358
C. joaquin.flores@al-enterprise.com

FOLIO. 23

Alcatel·Lucent Enterprise

CARTA DE DISTRIBUIDOR AUTORIZADO

Instituto Nacional para la Educación de los Adultos
Invitación a cuando menos Tres Personas
Procedimiento No. IA-11-MDA-011MDA001-N-59-2024
Nombre del licitante: REISCOM, S.A. DE C.V.
Fecha: 29 de mayo de 2024

Por medio del presente y en el marco del proyecto de referencia, me dirijo a usted a efecto de informarle que Reiscom S.A. de C.V. ha cumplido con los procedimientos requeridos por Alcatel-Lucent Enterprise y es un DISTRIBUIDOR ACREDITADO, AUTORIZADO Y CERTIFICADO para vender, instalar y soportar las soluciones tecnológicas de nuestra marca desde hace mas de 19 años.

Reiscom S.A. de C.V. cuenta con Ingenieros Calificados y Certificados para el manejo de los equipos de Alcatel-Lucent Enterprise , instalados en el en las oficinas del INEA.

Sin otro particular, quedo a sus órdenes.

Atentamente,

Joaquin Flores Tecillo
Channel Sales Leader
Alcatel Lucent Enterprise México
M. 5544993358
C. joaquin.flores@al-enterprise.com

Alcatel·Lucent Enterprise

CARTA DE EQUIPOS OFERTADOS

Instituto Nacional para la Educación de los Adultos
Invitación a cuando menos Tres Personas
Procedimiento No. IA-11-MDA-011MDA001-N-59-2024
Nombre del licitante: REISCOM, S.A. DE C.V.
Fecha: 29 de mayo de 2024

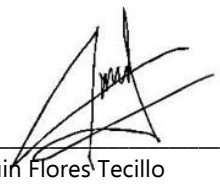
Por medio del presente y en el marco del proyecto de referencia, me dirijo a usted a efecto de informarle la lista de los equipos que forman parte de la propuesta de la empresa Reiscom S.A. de C.V. para cada una de las partidas descritas en el presente anexo técnico y que se certificará la configuración de dichos equipos.

1. Teléfono IP Marca Alcatel-Lucent Modelo Ale-20 (terminal IP básica)
2. Teléfono IP Marca Alcatel-Lucent Modelo 8088 (terminal IP ejecuttiva)
3. Licenciamiento para usuarios IP para conmutador Marca Alcatel-Lucent modelo OXO
4. Tarificador VCC

Reiscom S.A. de C.V. cuenta con Ingenieros Calificados y Certificados para el manejo de los equipos de Alcatel-Lucent Enterprise , instalados en el en las oficinas del INEA.

Sin otro particular, quedo a sus órdenes.

Atentamente,



Joaquin Flores Tecillo
Channel Sales Leader
Alcatel Lucent Enterprise México
M. 5544993358
C. joaquin.flores@al-enterprise.com

FOLIO. 25

Alcatel·Lucent Enterprise

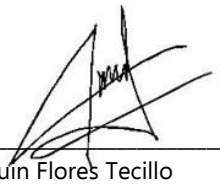
CARTA DE EXISTENCIA DE REFACCIONES

Instituto Nacional para la Educación de los Adultos
Invitación a cuando menos Tres Personas
Procedimiento No. IA-11-MDA-011MDA001-N-59-2024
Nombre del licitante: REISCOM, S.A. DE C.V.
Fecha: 29 de mayo de 2024

Por medio del presente y en el marco del proyecto de referencia, me dirijo a usted a efecto de informarle que la empresa Reiscom S.A. de C.V. y Alcatel-Lucent Enterpriser cuentan con la infraestructura técnica, de servicio y que garantizamos la existencia de refacciones para el mantenimiento de los bienes objeto del arrendamiento, durante la vigencia del contrato de arrendamiento.

Sin otro particular, quedo a sus órdenes.

Atentamente,



Joaquín Flores Tecillo
Channel Sales Leader
Alcatel Lucent Enterprise México
M. 5544993358
C. joaquin.flores@al-enterprise.com

Alcatel·Lucent Enterprise

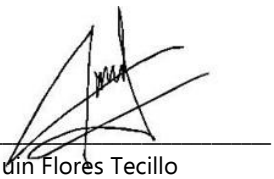
CARTA DE NO ANUNCIO DE FIN DE VIDA

Instituto Nacional para la Educación de los Adultos
Invitación a cuando menos Tres Personas
Procedimiento No. IA-11-MDA-011MDA001-N-59-2024
Nombre del licitante: REISCOM, S.A. DE C.V.
Fecha: 29 de mayo de 2024

Por medio del presente y en el marco del proyecto de referencia, me dirijo a usted a efecto de informarle que manifiesto que los equipos objeto del arrendamiento, no tendrán un anuncio de fin de vida ni anuncio de fin de mantenimiento durante la vigencia del contrato de arrendamiento.

Sin otro particular, quedo a sus órdenes.

Atentamente,



Joaquín Flores Tecillo
Channel Sales Leader
Alcatel Lucent Enterprise México
M. 5544993358
C. joaquin.flores@al-enterprise.com

FOLIO. 27

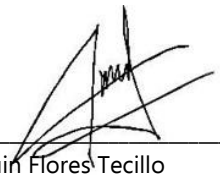
CARTA DE PERSONAL CERTIFICADO

Instituto Nacional para la Educación de los Adultos
Invitación a cuando menos Tres Personas
Procedimiento No. IA-11-MDA-011MDA001-N-59-2024
Nombre del licitante: REISCOM, S.A. DE C.V.
Fecha: 29 de mayo de 2024

Por medio del presente y en el marco del proyecto de referencia, me dirijo a usted a efecto de informarle que la empresa Reiscom S.A. de C.V. cuenta con Ingenieros Calificados y Certificados para la instalación, configuración y puesta a punto de los equipos de Alcatel-Lucent Enterprise instalados en las oficinas del INEA y propuestos en la presente licitación.

Sin otro particular, quedo a sus órdenes.

Atentamente,



Joaquin Flores Tecillo
Channel Sales Leader
Alcatel Lucent Enterprise México
M. 5544993358
C. joaquin.flores@al-enterprise.com

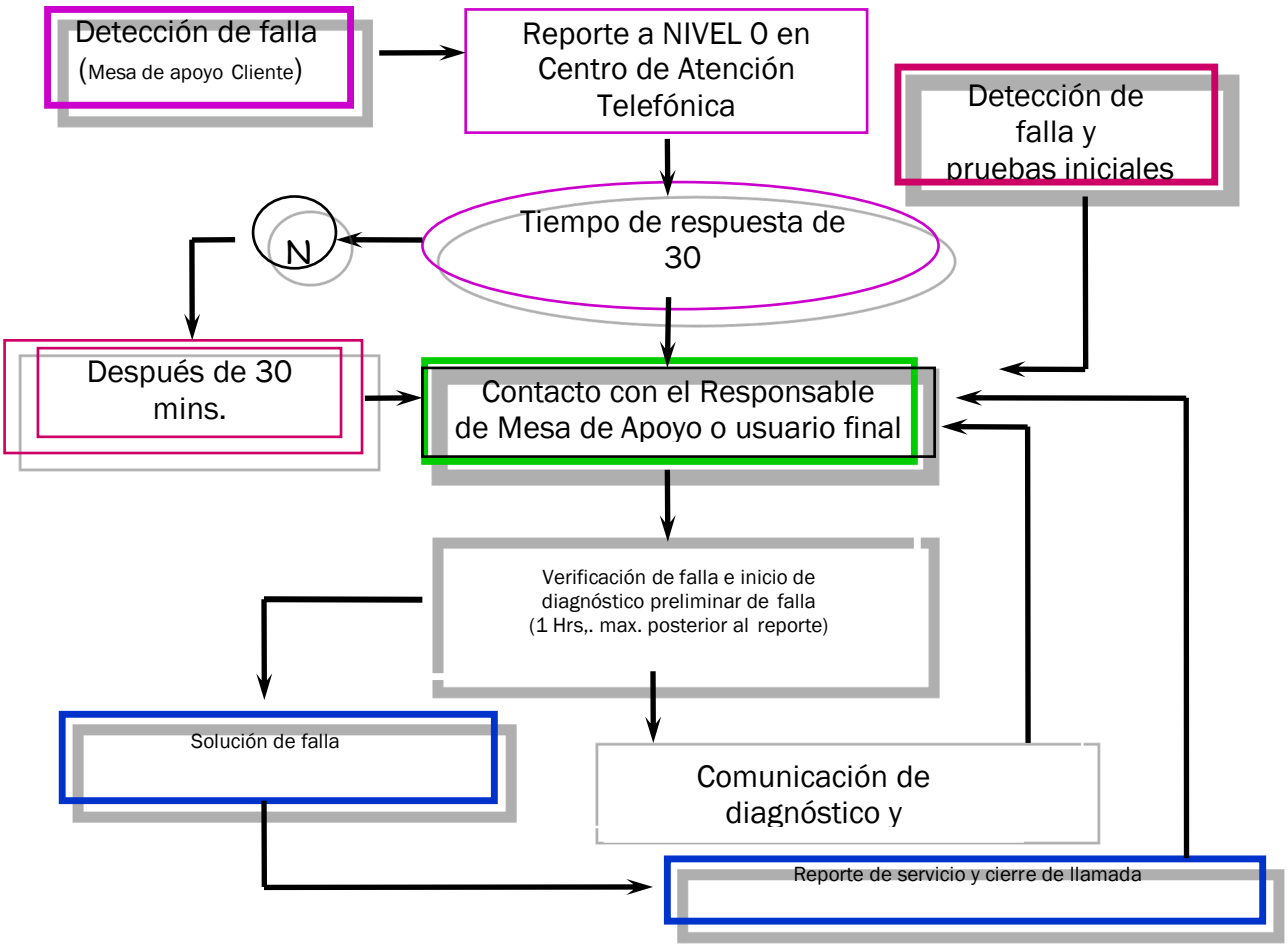
Vanguardia Tecnológica Para Su Empresa

METODOLOGÍA PRESTACIÓN DE SERVICIOS
Y MATRIZ DE ESCALAMIENTO.

Ciudad de México, a 29 de mayo de 204.

Instituto Nacional para la Educación de los Adultos
Invitación a cuando menos Tres Personas
Procedimiento No. IA-11-MDA-011MDA001-N-59-2024
Nombre del licitante: REISCOM, S.A. DE C.V.
Fecha: 29 de mayo de 2024

Asunto: **Metodología para la atención, seguimiento y escalación de los servicios**



Vanguardia Tecnológica Para Su Empresa

Metodología para la atención y seguimiento de los mantenimientos correctivos y preventivos, así como los servicios de garantía, que incluya lo especificado en el Anexo No. 1

TOMA DE REQUERIMIENTOS

La toma de requerimientos puede realizarse por dos vías principales:

1. Por medio del Administrador del proyecto.
2. Por medio del Portal Electrónico para seguimiento del proyecto.

En la última hoja se muestra los datos del personal responsable e involucrados en el proyecto y se indica como primer escalafón al Call Center:

TOMA DE REQUERIMIENTOS

La toma de requerimientos puede realizarse por dos vías principales:
El cliente, al momento de levantar el reporte, por cualquiera de los medios mencionados en la tabla anterior, deberá proporcionar la siguiente información:

- Nombre de la persona que registra la órden y/o ticket.
- Número telefónico en el cual pueda ser contactado.
- Descripción del requerimiento, incidente o del servicio solicitado.
- Dirección en donde se requiere el servicio.

En caso de que el cliente no obtenga respuesta en un tiempo de 15 minutos por parte del Centro de Servicio a Clientes, podrá ir directamente al siguiente nivel de escalamiento, según la matriz que se muestra más adelante en este documento.

Una vez registrada la llamada en el Centro de Atención, el personal que reciba la llamada informará al cliente el número de órden/ticket asignado así como la hora y fecha de registro de esta.

Hecho lo anterior, este número será turnado al personal correspondiente para su atención y seguimiento.

LEVANTAMIENTO DE REQUERIMIENTOS VIA WEB

Requerimientos:

El cliente debe contar con conexión a Internet y tener instalado un web browser como Internet Explorer, Google Chrome, Mozilla Firefox.

Pasos:

1. Tener a la mano:
   - Detalle del requerimiento

- Localidad donde se requiere la atención
- Nombre de los responsables de la localidad

2. Acceder a la página web. www.reiscom.com
3. Seleccionar la opción SOPORTE (Voz, Datos, Firrewall, Cableado Estructurado)

A continuación, se describen los campos contenidos en cuestionario para la apertura de reportes:

1. Nombre del Contacto: Contiene el nombre de la persona que está solicitando el servicio, y que será el punto de contacto para el seguimiento de la atención de este.
2. Correo Electrónico: Se deberá proporcionar una cuenta de correo electrónico para establecer contacto, y será el correo al cual se enviará la notificación de apertura del reporte.
3. Teléfono: Se debe proporcionar un número de teléfono que servirá para establecer contacto.
4. Tipo: Se define el tipo de servicio que se está solicitando, la opción deseada se puede elegir de un menú desplegable.
5. Asunto: Solicitud de servicio que se está realizando.
6. Descripción breve del Asunto: Una descripción breve de la solicitud de servicio que se está realizando.
7. Descripción: Realizar una descripción más detallada del incidente o requerimiento reportado.
8. Antecedentes: Mencionar si existe algún antecedente relacionado con el servicio que se está solicitando.

Teléfonos de atención a Clientes y Niveles de Escalación. (TOMA DE GOBIERNO)

La oficina de proyectos, (PMO por sus siglas en inglés Project Management Office) seguirá el procedimiento establecido para proporcionar la dirección del proyecto, estandarizando y monitoreando los procedimientos para asegurar la entrega del servicio y entregables comprometidos en esta propuesta.

Alcance

La extensión, diversidad y características especiales de la implementación de proyectos generan una gran variedad de requerimientos y servicios.

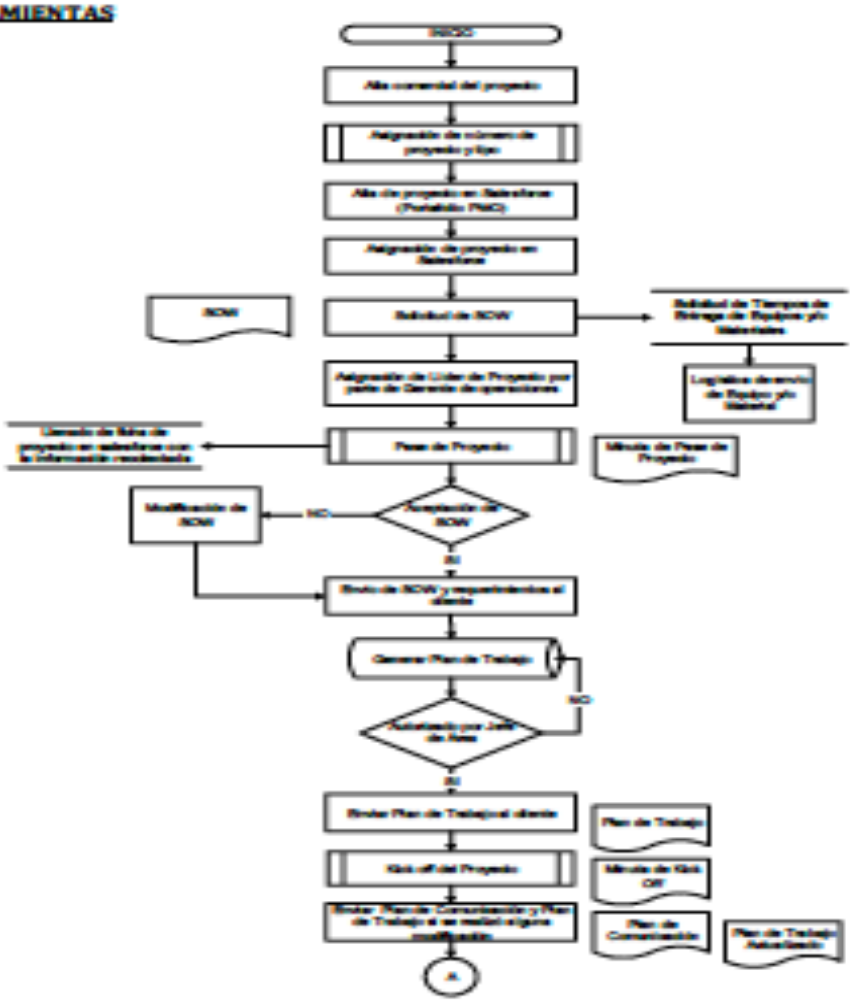
Los requerimientos del cliente involucran varios procedimientos de instalación y tecnologías, cada uno de ellos con diferente origen de fabricación, diferentes tiempos de producción, diferentes condiciones de entrega y transporte, así como diferentes prerrequisitos de implementación en materiales y recursos.

Vanguardia Tecnológica Para Su Empresa

El proceso descrito en este documento genera un análisis y soluciones que nos ayudan a construir una relación estratégica con las aéreas involucradas que deberán realizar una visión anticipada de los requerimientos para:

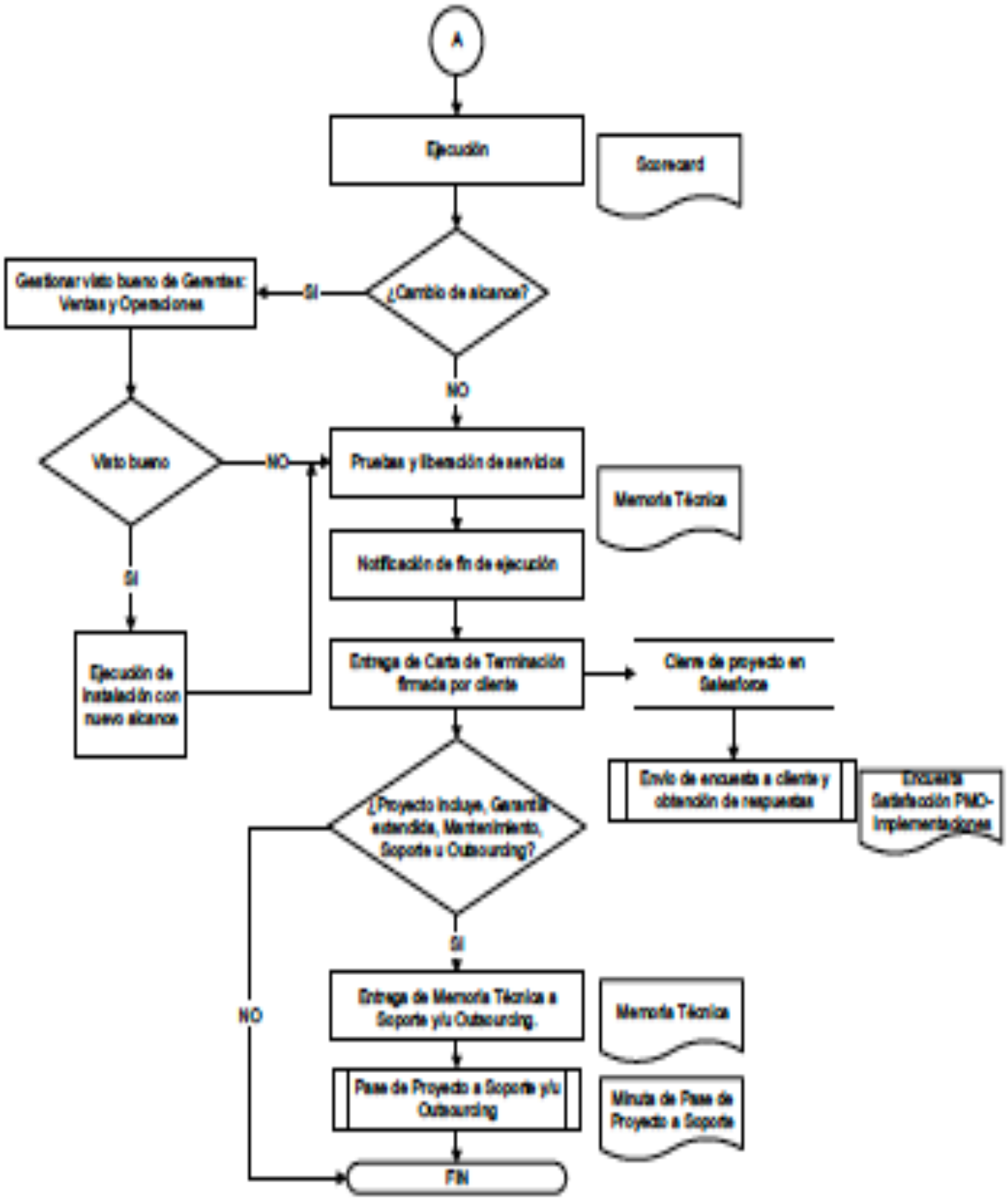
1. Satisfacer las expectativas del cliente.
2. Llevar una secuencia ordenada de actividades con las áreas involucradas, considerando sus tiempos de ejecución.
3. Tener un apropiado dimensionamiento de recursos.
4. Realizar una apropiada previsión, tanto de materiales, como de los recursos de instalación y prueba, logrando, por consiguiente, el control del proyecto.

PROCESO Y HERRAMIENTAS



ReisCom, S.A. de C.V.
Atlapulco 6 A Col. Vergel del Sur.
Del. Tlalpan, C.P.14340 Ciudad de México.
Teléfonos: 52643536 / 52643871

Vanguardia Tecnológica Para Su Empresa



Vanguardia Tecnológica Para Su Empresa

Detalle del proceso y herramientas

Inicio

Alta de proyecto

Por medio de un correo electrónico Ventas reporta el alta de proyecto, con el formato establecido, el cual contiene la información básica para dar de alta el proyecto en la PMO.

Asignación de número de proyecto y tipo.

Por medio de un correo electrónico la Administración de Proyectos y Cobranza asigna y/o confirma el alta del proyecto en la base de datos de Proyectos.

Alta de proyecto (Portafolio de la PMO).

Las administradoras de ventas realizan el alta de proyecto en el portafolio de PMO realizando su integración a la base de datos, donde hacen el llenado de la información.

Asignación de proyecto.

Se hace la asignación de Project Manager que dará seguimiento al proyecto, el responsable de esta asignación es el administrador del área de la PMO.

El Project Manager asignado deberá anunciar a todos los involucrados a través de un correo electrónico el alta de proyecto en el portafolio de la PMO. Esto dispara el proceso que permitirá dar un seguimiento a la gestión del proyecto en todas sus fases, con la intención de lograr una dirección de proyectos eficaz con un plan coordinado. El resultado será una sinergia de todas las áreas que permita minimizar riesgos y desviaciones.

Solicitud de SOW (Scope of Work).

Por medio de un correo electrónico se solicita al ingeniero de preventa, designado al proyecto, el SOW (documento con la justificación y los alcances) para enviarlo al Gerente de Operaciones. En paralelo se solicita el tiempo de entrega de los materiales y/o equipo al Gerente de Compras.

Planeación.

Asignación de Líder de Proyecto
Una vez compartido el SOW al gerente de operaciones, asignará un líder de proyecto (LP), según las habilidades y disponibilidad.

Pase de proyecto.

El Project Manager organiza una reunión en la que convoca a:
El Ingeniero de diseño (participación obligatoria)
El líder de proyecto (participación obligatoria)

El ejecutivo comercial (participación obligatoria)
El gerente de operaciones (participación opcional)
El jefe de área de ingeniería/preventa y el jefe de implementaciones (participación opcional) Área de logística (participación opcional)

Dicha reunión tiene la finalidad de validar la factibilidad operativa del proyecto, alcance, equipo vendido, requerimientos hacia el cliente, riesgos y fechas compromiso. Los acuerdos y compromisos obtenidos de este pase de proyecto quedaran asentados en una minuta llamada “Minuta de Pase de Proyecto”.

Llenado de la ficha de proyecto
Se complementa la información obtenida a lo largo del proceso como fechas, nombres de recursos, días e ingenieros estimados para la implementación, ejecutivo de ventas, estatus, actividades de plan de trabajo para graficar en Gantt, subir documentos relacionados al proyecto, etc. (Esta información será actualizada a lo largo de la duración del proyecto).

Envío de SOW y requerimientos a cliente.
Ya que todas las áreas involucradas tienen conocimiento de los alcances del proyecto, a través de un correo se envía al cliente el SOW junto con los requerimientos y se solicita disponibilidad para programar la junta de Kick off.

Plan de trabajo
El PM elabora en Microsoft Project el plan de trabajo por el que se regirán las actividades de la implementación, en este se definen tiempos y prioridades de cada actividad. Los tiempos y actividades son definidos con apoyo del líder de proyecto o jefe de área.
Este plan se envía al cliente antes de la junta kick off para que tenga oportunidad de revisarlo.

Kick off del Proyecto
El PM asignado convoca a una reunión en la que se invitará a:
Cliente (participación obligatoria)
El líder de proyecto (participación obligatoria)
El ejecutivo comercial (participación obligatoria)
El gerente de operaciones (participación opcional)
El jefe de área de ingeniería/preventa y el jefe de implementaciones (participación opcional)
El Ingeniero de diseño (participación opcional)

El objetivo de la reunión es definir un mismo criterio sobre el alcance del proyecto, explicar requerimientos y/o confirmarlos y que el ejecutivo de cuenta obtenga el visto bueno sobre el SOW.

El PM elaborará una minuta con los acuerdos y compromisos generados a lo largo de la reunión, documento que se llamará “Minuta de Kick off”.

Plan de comunicación

El PM asignado elabora como documento formal el plan de comunicación, el cual es la manera de estructurar la fluidez de la información, definir la estructura organizacional del personal involucrado y definir los medios y canales que se utilizarán para una comunicación adecuada.

Logística

Con la suficiente anticipación el LP o el PM (con el visto bueno previo del LP o el jefe de área de implementaciones) libera los materiales y/o equipos para ser entregados en tiempo y forma en el sitio indicado por el cliente.
El área de logística realizará la entrega del material y/o equipos en la fecha que se le indique y se le tendrán que proporcionan los siguientes datos:

1. Dirección completa con Código Postal.
2. Nombre y número del contacto que recibe.
3. Horario de atención.

Ejecución

Ejecución de instalación

El área de implementación es responsable de esta fase. El líder de proyecto aplica los métodos mantenimientos correctivos y preventivos de acuerdo al alcance del proyecto.
El líder de proyecto, bajo la supervisión de su Gerente o del Jefe de área, realizará la los trabajos correspondientes para cumplir con los requerimientos, siempre en la fecha y hora comprometida con el cliente.

Cambio de alcance

El Líder de proyecto o Jefe de Área reportará a la PMO y a todos los involucrados cualquier cambio de alcance (previamente definido en el SOW) para definir un acuerdo interno y con el cliente sobre si se ejecuta o no el nuevo alcance.

Monitoreo y control

Envío de Scorecard (Reporte de avances)
En esta fase el PM será el encargado de elaborar y enviar semanalmente el Scorecard con los avances o riesgos que le proporcione el líder de proyecto o jefe de área.
El Scorecard se tendrá que enviar por correo por medio de una liga de Salesforce donde previamente se habrá guardad, siendo los remitentes:

- Cliente (s)

- Dirección
- Gerente de preventa/PMO
- Gerente de operaciones
- Gerente de ventas
- Jefe del Área de PMO

Cierre

Notificación de fin de ejecución del proyecto

Una vez que las actividades de ejecución hayan concluido, el PM deberá enviar un aviso a los stakeholders notificando que las actividades fueron concluidas satisfactoriamente.

Entrega de Memoria Técnica

La memoria técnica del proyecto es la recopilación de todos los datos e información que respaldan el proyecto, en ella se encuentra el inventario de los equipos, diagramas, configuraciones, fichas técnicas de equipos y responsivas de usuarios y contraseñas. Su elaboración es responsabilidad del líder de proyecto y la revisión del correcto formato la realiza el PM para después enviarla al cliente en digital.

Nota: Si ésta no es entregada en el tiempo establecido, se escalará con el jefe inmediato para que no se vuelva una dependencia de cierre del proyecto.

Entrega de carta de terminación (Acta entrega-recepción)

Finalizada exitosamente la implementación el PM será el encargado de elaborar y conseguir la firma del cliente en la carta de terminación. Se podrá tener el apoyo del instalador si se encontrara en sitio y fuera más práctico conseguir la firma.
Una vez teniendo la carta firmada, se enviará a los stakeholders.

Cierre de proyecto.

Cuando ya no hay pendientes operativos ni administrativos se puede cerrar un proyecto en Salesforce, una vez cumpliendo con las siguientes premisas:

- Tener Memoria Técnica aceptada por el cliente.
- Tener Carta de Terminación firmada por el cliente principal.
- Tener certificados cuando aplique (solo aplica para proyectos de cableado).

ENTREGA DE SOPORTE TÉCNICO

MANTENIMIENTOS PREVENTIVOS

Objetivo

Vanguardia Tecnológica Para Su Empresa

Asegurar que los servicios se mantengan en óptimas condiciones de operación al realizar los mantenimientos preventivos y actividades acordadas con el cliente según lo contratado.

Impacto
Se suspenderán los servicios de acuerdo al calendario de actividades establecido previamente con el cliente. El periodo de suspensión de servicios está definido en la ventana de tiempo solicitada en el plan de trabajo entregado previamente a la ejecución de trabajos.

Justificación
El servicio de mantenimiento preventivo debe realizarse previo acuerdo con el cliente y de acuerdo a sus necesidades operativas con el fin de garantizar el óptimo desempeño de sus servicios.

Programación de Eventos de Manteamiento Preventivo
El plan de trabajo que se programará de acuerdo a las necesidades del cliente, dando seguimiento al plan de desarrollo de los objetivos alcanzables por parte del cliente y de Reiscom.

Administración-Distribución del Trabajo
Se contará con personal responsable para llevar a cabo las actividades de mantenimiento en cada localidad. También se requerirá un responsable en Oficinas Centrales del cliente durante los trabajos, para apoyo en accesos y validación de servicios.

Ejecución del mantenimiento Preventivo

Actividades Previas

1. Identificación del cableado conectado en los equipos.
2. Desconexión de cableado/servicios.
3. Realizar pruebas de desempeño para verificar posibles fallas.
4. Identificar y corregir la falla.
5. Realizar nuevas pruebas de desempeño para validar servicios.
6. Reconexión de servicios.
7. Validación de servicios.

Actividades de Reporte

- Elaboración de Reporte de Mantenimiento Preventivo de acuerdo al evento.
- Entrega de Reporte Mantenimiento Preventivo.

Cierre de actividad y documentación

Finalización

El cliente realizará las pruebas que considere pertinentes y adecuadas para la validación de sus servicios. Una vez realizadas estas pruebas deberá firmar la orden de servicio que respaldará el mantenimiento realizado.

Reporte de servicio

La información obtenida durante los mantenimientos preventivos se entregará como parte de la actualización de la memoria técnica, tomando como base y referencia la memoria del mantenimiento preventivo realizado por última vez.

Las actividades dentro de fechas propuestas a validar con el cliente se realizarán en los horarios de trabajo autorizados por el responsable de otorgar la ventana de tiempo.

MANTENIMIENTOS CORRECTIVOS

Los mantenimientos correctivos hacen referencia a las tareas que se deben llevar a cabo para la atención y solución de un incidente relacionado con la infraestructura de un cliente. Una de las principales tareas a realizar por el personal asignado en el proyecto, será la atención de incidentes y problemas reportados a través de la mesa de servicio siguiendo las principales actividades de los procesos de atención de Incidentes y Atención de problemas. Todos los incidentes y problemas deberán ser documentados en la herramienta de la mesa de servicios para su seguimiento y cierre, así como para la medición del cumplimiento de SLA’s acordados con el cliente.

Objetivos

- Asistencia telefónica.
- Asistencia en sitio en caso de requerirse.
- Diagnóstico del problema.
- Todo incidente que se presente en el ambiente productivo, deberá resolverse de la manera más rápida y eficaz posible.
- Solucionar el problema rápida y eficazmente, de acuerdo con los SLAs establecidos. Consistirá en la reparación y/o remplazo de las partes dañadas cuando ocurra la falla.

Vanguardia Tecnológica Para Su Empresa

8008301312 **5552643536** **5552643871**	**Call Center Reiscom** **Atención las 24 hrs. del día** **Tiempo de respuesta:** **Inmediato.**
Cel. 55 54048390 **Oficina: 55 52643536**	**José Antonio Flores Ascención** **Sub-Gerente de Redes** **Contactar después de 30 minutos de levantado el reporte**
Cel. 55 59954579 **Oficina: (55) 52643536**	**Salvador Flores Jimenez** **Gerente de Redes** **Contactar después de 30 minutos de levantado el reporte**
Cel. 55 55069384 **Oficina: (55) 52643536**	**Javier Murillo** **Director de Operaciones** **Contactar después de 1 hora de levantado el reporte**
Cel. 55 22741092 **Oficina: (55) 52643871**	**Antonio Rojas** **Director General** **Contactar después de 2 horas de levantado el reporte**

A t e n t a m e n t e

ReisCom, S.A. de C.V.
Ing. Francisco Javier Murillo Pantoja
Representante Legal

Vanguardia Tecnológica Para Su Empresa

CARTA ORIGEN

Instituto Nacional para la Educación de los Adultos
Invitación a cuando menos Tres Personas
Procedimiento No. IA-11-MDA-011MDA001-N-59-2024
Nombre del licitante: REISCOM, S.A. DE C.V.
Fecha: 29 de mayo de 2024

Me refiero al procedimiento **Invitación a cuando menos Tres Personas** No. **IA-11-MDA-011MDA001-N-59-2024** en el que mi representada, REISCOM, S.A. DE C.V. participa a través de la proposición que se contiene en el presente sobre.

Sobre el particular, manifieste que los equipos que oferto y suministraré son nuevos, no armados, no re-manufacturados y de modelos recientes (máximo dos años), especificando la fecha de inicio de comercialización del equipo.

ALE-20 EDICION 5	INICO DE COMERC IALIZACIÓN: 17 DE MAYO DE 2024
IP DESKTOP 8088 VERSIÓN R500.A3.065.1.3592	INICIO DE COMERCIALIZACIÓN: 15 DE ENERO DE 2024

Protesto lo necesario

Francisco Javier Murillo Pantoja
Representante Legal

Alcatel·Lucent Enterprise

Release Note	ALE Essential Deskphones

TC3073 ed.05 Release R300 and above

Technical Release Note for ALE DeskPhones ESSENTIAL ALE-20/20H ALE-30/30H R300 and above

Technical Release Notes of ALE DeskPhones ESSENTIAL: ALE-20 ALE-20H ALE-30 ALE-30H R300 and above.

Revision history

Edition 1: October 10, 2023	creation of the document
Edition 2: December 21, 2023	update for version 1.40.20
Edition 3: April 23, 2024	update for version 1.40.30, 1.40.31, 1.40.32 (1.40.31 is the factory version since April 2024, ALE 4K certificate inside)
Edition 4: May 7, 2024	update for version 1.50.08 (1st version for R310, introduction of security fix. R310 new features description will be in next edition)
Edition 5: May 17, 2024	update for R310 new features delivered in version 1.50.08

Alcatel·Lucent Enterprise

Release Note	8088 Android NOE

TC2347 ed.27 Release 500.0

Technical Release Notes For 8088 ANDROID NOE Smart Deskphone

Technical Release Notes of version R500.

Revision History

Edition 1: November 1, 2017	creation of the document
Edition 2: January 22 2017	new release R301 A3.025.2 (BT functional)
Edition 3: February 2 2018	release A3.025.4 bug fixes for only phone 4GB with ALE BT.
Edition 4: April 5 2018	release A3.027.1 for phone 4GB v1 and 16GB v2 with RTX BT.
Edition 5: June 18 2018	release A3.033.2
Edition 6: January 15, 2019	release A3.048.3.1665 OXE, A3.047.3.1627 OXO, video through rainbow application
Edition 7: March 11, 2019	release A3.049.3.1726 maintenance version (OXO, OXE) + new features for Japan (OXE) market
Edition 8: March 28, 2019	maintenance version A3.049.4.1727
Edition 9: June 4, 2019	maintenance version R304:A3.050.5.2052
Edition 10: July 16, 2019	maintenance version R304:A3.051.2.2145
Edition 11: August 8, 2019	maintenance version R304:A3.052.1.2174 for OXE only
Edition 12: October 23, 2019	maintenance version R304:A3.052.2.2220 for OXO only (OCO, OCE)
Edition 13: December 20, 2019	maintenance version R304:A3.053.6.2302 for OXE M3/M4 (BT headsets)
Edition 14: March 16, 2020	maintenance version R304:A3.054.3.2380 for OXE
Edition 15: April 20, 2020	maintenance version R304:A3.054.4.2403 for OXE and new custo tool (2.1.8) for 8088.
Edition 16: October 19, 2020	first release R500 version R500:A3.061.8.3108 for OXE M5 introducing the IPV6 on 8088, for OXO as a maintenance version (bug fixing)
Edition 17: November 17, 2020	maintenance version R500.A3.063.2.3239 (for OXE, mainly fixes in PCS mode) configuration)
Edition 18: March 2, 2021	maintenance version R500.A3.063.4.3327 (5.06.34) for OXE
Edition 19: June 9, 2021	maintenance version R500.A3.063.5.3352 (5.06.35) for OXE, OXO (OCO, OCE): USB headsets supported Maintenance version R500.A3.063.6.3416 (5.06.36) for OXE only
Edition 20: October 8, 2021	Maintenance version R500.A3.064.0.3457 (5.06.40) for OXE, OCO, OCE (support of the new sensitive bar and new Power Management IC provided in the flash image for these phones with new component to replace obsolete one)

Edition 21: December 22, 2021	Maintenance version R500.A3.064.2.3472 (new u-boot update to fix ethernet issue caused by new PMIC F2, new camera support, Bluetooth wideband support)
Edition 22: June 7th, 2022	Maintenance version R500.A3.064.5.3500 (support and it fixes also the sense bar issue)
Edition 23: August 8th, 2022	Maintenance version R500.A3.064.6.3511(Bluetooth wideband support for ALE BT handset and BT headsets)
Edition 24: October 7th, 2022	Maintenance version R500.A3.064.7.3519 (one fix relative to popup “no enough space available on the phone“)
Edition 25: July 6th 2023	Maintenance version R500.A3.064.9.3557 (one fix relative to loss of connection after an upgrade)
Edition 26: August 7th 2023	Maintenance version R500.A3.065.0.3567 (one fix relative to loss of connection after an upgrade (due to last fix))
Edition 27: January 15th 2024	Maintenance version R500.A3.065.1.3592 (audio improvements: audio delay when taking a call)

Alcatel·Lucent Enterprise

Teléfonos de escritorio ALE DeskPhones: gama Essential

La gama Essential de teléfonos de escritorio ALE DeskPhones de Alcatel-Lucent Enterprise ofrece una rica experiencia de comunicación con las soluciones de Alcatel-Lucent Enterprise. Los cuatro modelos (ALE-20, ALE-20h, ALE-30 y ALE-30h) tienen un diseño compacto y una navegación intuitiva.

Estos modelos de grandes prestaciones ofrecen la mejor relación calidad-precio. Disfrute de una calidad de audio de banda ancha desde el terminal o en modo manos libres. Los puertos USB-A y USB-C permiten conectar cómodamente unos auriculares.

Con su gran pantalla, teclas de software y un botón de navegación tetradireccional, los teléfonos de escritorio de la gama Essential simplifican la experiencia del usuario. Contacte rápida y fácilmente con colegas y clientes utilizando el teclado alfabético opcional.

ALE-30/30h DeskPhone con teclado ALE-10

ALE-20h y ALE-30h ofrecen una conectividad digital e IP híbrida; además, le permiten aprovechar su infraestructura actual y, al mismo tiempo, evolucionan con sus necesidades. Realice una transición fluida de la tecnología digital a la IP y proteja su inversión. Despliegue de forma segura la gama Essential en cualquier entorno empresarial, desde la centralita local hasta la implementación en la nube en los servidores de Alcatel-Lucent Enterprise.

Puede desplegar los teléfonos en casa o en la oficina usando servidores de comunicación ALE. Los modelos ALE-20 y ALE-30 incluyen dos puertos RJ-45 Gigabit Ethernet. Los modelos ALE-20h y ALE-30h integran un puerto RJ-45 IP y digital con modo de detección automática.

Funciones	Ventajas
Comunicaciones empresariales de Alcatel-Lucent Enterprise	Acceda a todos los servicios enriquecidos e innovadores de las plataformas de comunicación de Alcatel-Lucent Enterprise
Teléfonos híbridos digitales e IP (ALE-20h/ALE-30h)	Aproveche su infraestructura actual y realice una transición fluida a IP conservando su inversión. Despliegue de largo alcance (hasta 800 m) en un solo par en modo digital.
Diseño compacto	Para usar en espacios abiertos, habitaciones de hoteles y hospitales o camarotes de cruceros.
Calidad de audio de banda ancha (ALE-20/ ALE-30, ALE-20h y ALE-30h en modo IP)	Gestione sus conversaciones cómodamente desde el terminal y el auricular, o bien en modo manos libres.
Teclado alfabético	Conecte fácilmente con sus colegas utilizando un teclado alfabético, disponible como opción.
Puertos USB-A y USB-C	Conecte unos auriculares para sus largas conversaciones diarias, o bien módulo adicional (EM200), admite hasta 3.
Consumo eléctrico	Disfrute de un bajo consumo de energía en digital o IP con PoE de clase1.
Despliegue sin intervención(zero-touch) en las soluciones Alcatel-Lucent Enterprise	Ahorre tiempo al desplegar y operar teléfonos en diferentes configuraciones, para Alcatel-Lucent OXO Connect, Alcatel-Lucent OXO Connect Evolution, Alcatel-Lucent OmniPCX® Enterprise. Configuración del cliente VPN con el servidor EDS.

Ficha técnica
Teléfonos de escritorio ALE DeskPhones



1

Modelos		ALE-20	ALE-30	ALE-20h	ALE-30h
Información destacada		2x Gigabit Ethernet, USB-A/C		Hybrid Digital/IP, USB-A/C	
		pantalla retroiluminada, 2x3 teclas programables	pantalla en color, 2x5 teclas programables	pantalla retroiluminada, 2x3 teclas programables	pantalla en color, 2x5 teclas programables
Pantalla	Retroiluminada de 2,8 pulgadas	•		•	
	A color de 3,5 pulgadas		•		•
Conectividad	USB-A	•	•	•	•
	USB-C	•	•	•	•
	RJ-45 FE/GE	-/•	-/•	•/-	•/-
	Puerto RJ-45 PC	•	•	•	•
	Auriculares/teclado RJ9	•/•[2]	•/•	•/•[2]	•/•
Características de Alcatel-Lucent Enterprise	Teclas contextuales	2x3	2x5	2x3	2x5
Audio	Banda ancha (modo IP)	•	•	•	•
	Altavoz full duplex (IP/digital)	•	•	•	•
	Supresión de ecos (IP/digital)	•	•	•	•
Accesorios	Teclado alfabético (ALE-10)	o	o	o	o
	Módulo de expansión en Color[3] (hasta 3 EM200)	o	o	o	o
	Kit de montaje en pared	o	o	o	o
Fuente de alimentación	PoE, alimentación a través de Ethernet	clase 1	clase 1	clase 1	clase 1
	PoDL, alimentación a través de línea digital			•	•
	Adaptador de alimentación local USB-C (opción)	o	o	o	o
	Consumo de energía en reposo/activo (sin USB)	1.2W / 1.6W	1.2W/1.8W	0.8W/1W	0.8W/1.2W

1 ALE-30 disponible en Q1/2024
2 Sólo en 3ML37020BB & 3ML37020BA
3 Adaptador de alimentación opcional necesario según el contexto digital o IP

• = incluido
o = opcional

Especificaciones técnicas

Características físicas

- Altura: 183 mm (7,2 pulgadas)
- Anchura: 207 mm (8,2 pulgadas)
- Profundidad: 35 mm (1,4 pulgadas)
- Peso: 806 g (1,78 lb) incluyendo el terminal y el soporte
- Color: gris
- Pies ajustables: 40° y 55°
- Kit de montaje en pared

Pantalla

- ALE-20 y ALE-20h: LCD de 2,8 pulgadas en blanco y negro, 64 x 128 píxeles, retroiluminación blanca
- ALE-30 y ALE-30h: LCD en color de 3,5 pulgadas, 240 x 320 píxeles

Teclas

- Navegador: navegación tetradireccional, teclas OK y Cancelar
- Teclas contextuales con leds:
  - ALE-20 y ALE-20h: 2 x 3
  - ALE-30 y ALE-30h: 2 x 5
- Teclas de función: colgar/descolgar, teclado marcador, silencio con LED, teclas de volumen +/-, manos libres con LED, 2 teclas personales con LED, rellamada, información y mensaje con LED
- Teclas programables:
  - OmniPCX Enterprise: hasta 72 teclas programables
  - OXO Connect y OXO Connect Evolution: hasta 40 teclas programables

Conectividad

- ALE-20 y ALE-30:
  - Puerto RJ-45 LAN: Gigabit Ethernet 10/100/1000
  - Puerto RJ-45 PC: conmutador Gigabit Ethernet 10/100/1000
- ALE-20h y ALE-30h:
  - Puerto RJ-45: Fast Ethernet 10/100 o línea digital UA
- ALE-20/ALE-20h, ALE-30/ALE-30h:
  - puerto RJ-9 para teclado alfabético opcional y depuración
  - Puerto RJ-9 para el auricular con cable
  - 1 x USB-C
  - 1 x USB-A (5 V, 100 mA)
  - Hasta 4,5 W (5 V, 900 mA) de potencia Boost o con un adaptador decorriente local

Fuente de alimentación

- Alimentación a través de Ethernet (IEEE 802.3af), clase 1
- Adaptador de corriente USB-C de 5V/2A opcional
- Adaptador de alimentación opcional 5V/3A USB-C PD
- Clasificación de ENERGY STAR®
- ALE-20:
  - Alimentación a través de Ethernet (PoE)
  - Consumo de energía en reposo/activo (sin USB): 1,2 W/1,6 W
- ALE-20h:
  - Alimentación a través de línea digital (PoDL)
  - Alimentación a través de Ethernet (PoE)
  - Consumo de energía en reposo/activo (sin USB): 0,8 W/1 W
- ALE-30:
  - Alimentación a través de Ethernet (PoE)
  - Consumo de energía en modo de espera/activo (sin USB): 1,2 W/1,8 W
- ALE-30h:
  - Alimentación a través de línea digital (PoDL)
  - Alimentación a través de Ethernet (PoE)
  - Consumo de energía en modo de espera/activo (sin USB): 0,8 W/1,2 W

Funciones de audio

- Terminal, auricular y manos libres de confort de banda ancha
- Compatibilidad con audífonos (HAC)
- Manos libres full-duplex
- Cancelación de eco acústico
- ALE-20 y ALE-30:
  - Códec OPUS (NB y WB)
  - G722
  - G711 (ley A y ley Mu)
  - G729 AB
- ALE-20h y ALE-30h:
  - G711 (ley A y ley Mu)
  - Detección de actividad de voz (VAD)
  - Generación de ruido de confort (CNG)
  - En modo IP:
    - Códec OPUS (NB y WB)
    - G722
    - G711 (ley A y ley Mu)
    - G729 AB

Red y aprovisionamiento

- ALE-20, ALE-30, ALE-20h y ALE-30h en modo IP
- DHCP e IP estática:
  - Configuración manual
  - Configuración de red mediante protocolo de configuración dinámica de host (DHCP)
  - IPv4/IPv6
- Compatibilidad con Calidad de servicio (QoS):
  - Etiquetado IEEE 802.1p/Q (VLAN)
  - TOS y DSCP de capa 3
  - Tickets de QoS
- LLDP-MED: cliente IEEE 802.1 AB/LLDPMED
  - Adquisición automática de VLAN
  - Gestión de PoE
  - Información de inventario
- Compatibilidad con Energy Efficient Ethernet 802.3 az

Protocolos y comunicaciones empresariales

- ALE-20/ALE-30 y ALE-20h/30h en modo IP: IP-NOE
- ALE-20h y ALE-30h en modo digital: NOE-UA
- Acceso a todas las funciones de comunicación de ALE desde:
  - Servidor de comunicación OmniPCX Enterprise
  - OXO Connect
  - OXO Connect Evolution: solo modo IP

Plataforma de aplicaciones abierta

- Soporte de aplicaciones XML (NOE-IP)
- Acceso al directorio corporativo mediante LDAP[1]

Seguridad

- ALE-20, ALE-30, ALE-20h y ALE-30h en modo IP
- Autenticación: básica o Digest, 802.1x
  - 802.1x Message Digest 5 (MD5)/TLS: para autenticación, gestión de certificados del cliente con implementación centralizada
  - Protección contra ataques de denegación de servicio (DoS): desbordamiento
  - Protección contra la suplantación de identidad ARP
- Transporte: TLS 1.2 y SRTP
  - Cifrado y autenticación del tráfico de señalización
    Cifrado del tráfico multimedia
    Compatibilidad con SCEP
- La entrega incluye el certificado X509v3 instalado.
  - Certificados para 802.1x EAP-TLS (certificados de Alcatel-Lucent o del cliente) para cifrado nativo (compatiblidad con NOE-DTLS)
- Compatibilidad con IP Sec VPN

Idiomas

- Asistencia multilingüe (menú): árabe, catalán, chino (simplificado), chino (tradicional), croata, checo, danés, neerlandés, inglés, inglés de Australia, inglés de Estados Unidos/Canadá, estonio, finés, flamenco, francés, francés de Canadá, francés de Suiza, alemán, alemán de Austria, alemán de Suiza, griego, hebreo, húngaro, italiano, italiano de Suiza, japonés, coreano, letón, lituano, noruego, polaco, portugués, portugués de Brasil, rumano, ruso, serbio, eslovaco, esloveno, español, sueco, taiwanés, tailandés, turco, valenciano.

1 disponible en próximas ediciones

Normas reguladoras

- Seguridad
  - ¬ IEC/EN 62368-1
  - ¬ UL/CSA 62368-1
- EMC
  - ¬ EN 55032 Clase B
  - ¬ 47 CFR Parte 15 B Clase B
  - ¬ ICES-003 Clase B
  - ¬ EN 55035
  - ¬ EN 61000-6-1 (Inmunidad para entornos residenciales comerciales)
  - ¬ EN 61000-6-2 (Inmunidad para entornos industriales)
  - ¬ EN 61000-6-3 (Emisión para entornos residenciales y comerciales)
  - ¬ entornos residenciales y comerciales)
  - ¬ EN 61000-6-4 (Emisión para entornos industriales)
  - ¬ IEC 60945 (Marítimo)
  - ¬ IEC 62236-4 (Ferroviaria)
  - ¬ IEC 60259 (IPX2)
  - ¬ EN 61000-3-2
  - ¬ EN 61000-3-3
- Telecomunicaciones
  - ¬ TIA / EIA 810-B, TIA 920.130-A-1, AS/CA S004
- Ayuda auditiva
  - ¬ FCC47 CFR Parte 68, Industria Canadá CS-03 Parte V, Australia AS/ACIF S040
- Diseño ecológico
  - ¬ 2009/125/CE, ROHS
  - ¬ 2011/65/UE, WEEE 2012/19/UE
  - ¬ REACH 1907/2006

Condiciones ambientales

- Temperatura: de -5 °C a +55°C
- Humedad relativa: del 5 % al 85 %
- Temperatura de almacenamiento: -25 °C/+70 °C
- Clase IP: IP22

Mantenimiento

- Modo Syslog, duplicación de puertos

El producto incluye

- Teléfono de escritorio con terminal y soporte
- Ficha de seguridad

Información de pedidos

- ALE-20 3ML37020BB
- ALE-30 3ML37030AB
- ALE-20h 3ML37020BA
- ALE-30h 3ML37030AA

Accesorios

- 3ML37010FR ALE-10 Teclado AZERTY
- 3ML37010DW ALE-10 Teclado QWERTY
- 3ML37010DE ALE-10Teclado QWERTZ
- 3MK27007AA Módulo de expansión EM200
- 3MK27008AA Kit de instalación mural
- 3MK08005xx Adaptador de corriente USB-C de 5V/2A
- 3ML37190xx 5V/3A USB-C PD Power Adapter
- 3AK21492AB 3M Cable Ethernet cat5 (x10)
- 3ML37001AA 3M cable de telefonía cat3 RJ45-RJ11 (x10)
- 3ML37005AA Microteléfono de repuesto
- Auriculares con cable:
  - ¬ 3MK08018AA AH 21 M II auricular premium monoaural 3,5 mm Jack/USB-A/C
  - ¬ 3MK08014AB AH 22 M II Premium auricular binaural 3,5 mm Jack/USB-A/C
- Auriculares inalámbricos:
  - ¬ 3MK37008AA Auriculares AH80 BT con dongle USB-A

Ejemplos de configuración

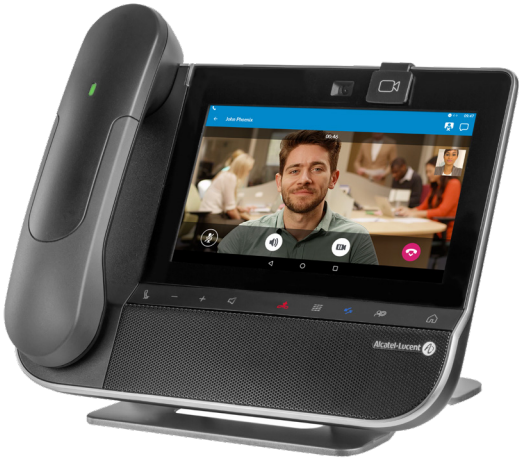
ALE-20/20h DeskPhone con Teclado Qwerty ALE-10 y Módulo de expansión EM200

ALE-30/30h DeskPhone con Teclado Qwerty ALE-10 y Módulo de expansión EM200

Alcatel·Lucent Enterprise

8088 Smart DeskPhone de Alcatel-Lucent

Alcatel-Lucent 8088 Smart Deskphone ofrece colaboración instantánea en vídeo a ejecutivos, gerentes y trabajadores de la información.



Este elegante y exclusivo teléfono ofrece una gran pantalla táctil de 7 pulgadas (17,78 cm) para la visualización de vídeo y una experiencia intuitiva. Cualquier pequeña sala de reunión se convierte en una sala de videoconferencia gracias a la cámara integrada y al audio de banda ancha.

El modelo 8088 también cuenta con un microteléfono Bluetooth y auriculares Bluetooth, para una movilidad inalámbrica de hasta 10 metros desde su escritorio.

Su plataforma Android proporciona a cualquiera la capacidad de implementar aplicaciones personalizadas y seguras. Con la aplicación de colaboración Alcatel-Lucent Rainbow, vea rápidamente quién está disponible y transforme, con un solo toque, cualquier llamada en una videoconferencia instantánea con colegas conectados a Rainbow desde cualquier dispositivo.

Funciones	Ventajas
Aplicación de colaboración Alcatel-Lucent Rainbow	Vea rápidamente quién está conectado, tan fácil como un solo toque para llamar a sus colegas conectados a Rainbow desde cualquier dispositivo.
Llamada de videoconferencia	Transforme cualquier sala de reunión en una sala de videoconferencia, con la pantalla táctil de 7" y la cámara HD integrada.
Aplicaciones Android de asistencia	Implemente aplicaciones personalizadas y seguras para todos los usuarios
Calidad de audio de banda ancha	Disfrute de una alta calidad de audio para una mayor comodidad
Coonectividad Bluetooth	Conecte un microteléfonol Bluetooth o unos auriculares Bluetooth para una movilidad inalámbrica de hasta 10 metros desde su escritorio.

Especificaciones técnicas

Datos mecánicos

- Peso: 1486 g (3,27 lb), microteléfono incluido
- Profundidad: 167 mm (6,57 in)
- Anchura: 252 mm (9,92 in)
- Altura: 204 mm (8,03 in)
- Color: Negro
- Base ajustable entre 25º y 60º
- Protección frente a infiltraciones (IP): 22

Pantalla

- Pantalla táctil TFT-LCD gráfica en color de siete pulgadas
- WVGA (Wide video graphics array): 800x480, formato 16:9
- Pantalla externa por medio de HDMI: hasta 1280x720
- Tecnología de pantalla táctil capacitiva
- Sensor de luz ambiental
- Retroiluminación de LCD:
  - ¬ Ajuste manual basado en un nivel definido por el usuario
  - ¬ Modo de ajuste automático del brillo en función de la luz ambiental y del nivel definido por el usuario

Conectividad

- LAN: Ethernet 10/100/1000
- PC a través de conmutador Ethernet 10/100/1000
- Conector de audio estéreo universa de 3,5 mm, 4 patillas, conforme al
- estándar de la CTIA (Cellular Telephone Industries Association)/AHJ (American Headset Jack)
- Dos puertos USB (1.1/2.0) para conectar una cámara externa, equipos de audio, cargar smartphones o conectar una memoria USB
- Conector RJ9 para auricular con cable (opcional)
- Bluetooth incorporado: compatible con auriculares, teléfonos, altavoces y manos libres
- Salida HDMI 1.4a, que permite replicar la pantalla y mostrar vídeo HD

Alimentación

- Power over Ethernet (PoE) 802.3AF
- Soporte de Clase 3

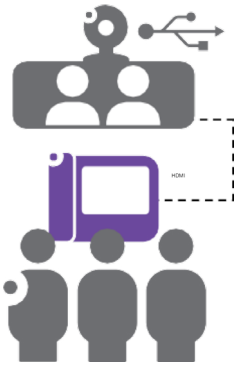
Audio

- Audio HD:
  - ¬ Altavoz de banda ancha
  - ¬ Teléfono Bluetooth de banda ancha
  - ¬ Auricular de banda ancha cómodo y con cable
- Altavoz de manos libres full duplex
- Cancelación de eco acústico
- Control de ganancia automático (AGC) para ajustar el volumen del audio y ofrecer comodidad mientras se está en una conferencia

Vídeo

- H264 Baseline Profile Level 3.0
- Picture-In-Picture (superposición de vista previa de uno mismo)
- Compensación de fluctuaciones en la alimentación
- Conexión/desconexión en caliente de cámaras USB externas
- Visualización de vídeo HD por medio de una salida HDMI
- Cámara HD interna:
  - ¬ 720p a 25 fps
  - ¬ 5 MP
- Obturador mecánico para ofrecer privacidad HDMI

Figura 1. Configuración de videoconferencia



Teclas y navegación

- Teclas sensibles con gestión de LED contextual:
  - ¬ Silencio
  - ¬ Volumen +/Volumen -
  - ¬ Selección de modo de audio: manos libres, altavoz, auriculares o teléfono
  - ¬ Colgar
  - ¬ Servicios de comunicación: comunicaciones activas, historial de llamadas, acceso a correo de voz e indicador de mensajes en espera
  - ¬ Teclado de marcación / teclado
  - ¬ Servicios y ajustes del usuario: vista de uno mismo en vídeo, enrutamiento, desbordamiento y suscripción de telefonía avanzada (incluidos bloqueo, supervisión, CLIR…)
  - ¬ Tecla de inicio que permite el acceso inmediato a la página y los menús de inicio
- Navegación mediante pantalla táctil
- Gestos para activar las funciones que se utilizan con más frecuencia, como marcación por nombre, controles de vídeo, salida HDMI y teclas programables

Gestión centralizada

- Protocolo de configuración dinámica de host (DHCP)/ Asignación automática de VLAN (AVA)
- Link Layer Discovery Protocol for Media Endpoint Devices (LLDPMED) (802.3 AB)
  - ¬ Extensiones: asignación de VLAN, gestión de PoE, inventario, geolocalización
  - ¬ HTTP/ HTTPS
- Actualización de software
  - ¬ Modo de actualización rápida: descarga de software en segundo plano. El dispositivo está disponible para el usuario también durante las llamadas de audio y de vídeo.
  - ¬ ~1 min. de falta de disponibilidad del dispositivo durante el arranque
  - ¬ Planificación por medio de OmniVista® 8770 Network Management System de Alcatel- Lucent
- Configuración del dispositivo basada en estándares de la empresa: gestión de la energía y configuración de servicios de telefonía, como altavoz de manos libres, Bluetooth, bloqueo automático, disponibilidad de accesorios de audio, gestión de audio y seguridad
- Interfaz de usuario personalizable (máscara, melodía, colores e imagen de fondo) utilizando la aplicación gráfica Smart-Custo for DeskPhone para crear una nueva máscara en el 8088 Smart DeskPhone
- Gestión de fecha y hora centralizada (Simple Network Time Protocol, SNTP)

Calidad de servicio

- 802.1 p/Q
- Punto de código de servicios diferenciados (DSCP)

Seguridad

- HTTPS para acceso por HTTP seguro
- 802.1x Message Digest 5 (MD5)/TLS: gestión de certificados del cliente (con implantación centralizada) para autenticación
- Protección contra ataques de denegación de servicio (DoS): desbordamiento
- Autenticación de mensajes de Protocolo de Inicio de Sesión (SIP) por medio de filtrado de IP
- Protección contra suplantación de direcciones mediante protocolo de resolución de direcciones (ARP)
- Estándar Transport Layer Security (TLS) 1.2
- Compatibilidad con algoritmo hash seguro (SHA)-2
- Cifrado de audio mediante SIP TLS y protocolo de transporte en tiempo real seguro (SRTP)

Internacionalización y localización

- Soporte para 29 idiomas y editores de métodos de escritura, como Pinyin, Katakana, Hiragana y Hangul

Accesibilidad

- • Compatibilidad con audífonos (HAC)
- LED intermitente para llamadas entrantes: visible desde las partes delantera y posterior

Servicios de comunicación

- Servicios de telefonía: controles para llamar, rechazar, consultar, mantener en espera, desviar, transferir e iniciar conferencia
- Gestión multilínea
- Registro de llamadas: perdidas, salientes y entrantes
- Marcación DTMF (multifrecuencia de doble tono)

Servicios de comunicaciones empresariales

- Realice, conteste y gestione conferencias de voz y de vídeo HD de banda ancha
- Identificación y presentación de imagen del llamante
- Servicios en llamada: desviar, añadir participantes, eliminar participantes, DTMF
- Acceso universal al directorio
  - ¬ Inicio de una sesión de audio o vídeo con una sola pulsación
  - ¬ Añada contactos a una lista de favoritos unificada entre dispositivos
  - ¬ Ver la imagen, telefonía en tiempo real, presencia y disponibilidad de contactos favoritos
- Identidad única entre dispositivos
  - ¬ Selección de reglas de enrutamiento definidas por el usuario
  - ¬ Enrutamiento a uno o varios dispositivos
  - ¬ Cambio rápido de sesión
  - ¬ Filtro de supervisión y captura de llamadas
  - ¬ Filtro Manager-Assistant (gerente/asistente)
  - ¬ Visualización y gestión de un historial de llamadas y de mensajes unificado entre dispositivos
  - ¬ Consulta y gestión de mensajería de voz visual unificada entre dispositivos
- Bloqueo y desbloqueo
- Supervivencia SIP:

- ¬ Recuperación automática en OmniPCX® Enterprise Communication Server (CS) o en OmniPCX Enterprise Passive Communication Server (PCS)
- ¬ Recuperación automática en servidores de terceros (programa AAPP) ¬ No es necesario reiniciar

Gestión de contactos

- Añadir, editar y eliminar contactos locales
- Gestión de listas de favoritos, centralizada con otros dispositivos

Productos compatibles

- Alcatel-Lucent OpenTouch® Multimedia Services, OpenTouch Business Edition, (desde la versión 2.1, incluido OmniVista 8770 Network Management System)
- OXO Connect y OXO Connect Evolution desde la versión 3.0 y superiores
- Desde OmniPCX Enterprise 12.1, ofrece la gama completa de servicios de telefonía disponibles en los reconocidos servidores de comunicaciones de Alcatel-Lucent, incomparables en términos de funcionalidad, prestaciones, fiabilidad y calidad de servicio.

Para obtener más información sobre las características y restricciones disponibles, consulte la guía del usuario 8088 Smart DeskPhone

Personalización basada en el usuario

- Reproductor de archivos de audio (MP3, WAV)
- Visor de imágenes y fotos (JPG, BMP, PNG)
- Acceso a opciones locales para:
  - ¬ Protector de pantalla u opciones definidas por el usuario
  - ¬ Melodías de timbre de llamada y notificación (más de 10 opciones)
  - ¬ Imagen de fondo u opciones definidas por el usuario
  - ¬ Máscaras de color
  - ¬ Gestión de equipos de audio
  - ¬ Preferencias del usuario (como página de inicio y retroiluminación)

Accesorios en el catálogo

- Teléfono cómodo de banda ancha, con cable
- Terminal Bluetooth
- Inyector PoE
- Adaptador de alimentación de 48 V
- Auriculares (para obtener una lista actualizada, consulte el catálogo)

Compatibilidad con aplicaciones de terceros

Se pueden implementar aplicaciones empresariales específicas en el 8088 Smart DeskPhone.

Alcatel·Lucent Enterprise

Alcatel·Lucent Enterprise

Alcatel-Lucent OXO Connect

Servidor de comunicaciones para las Pymes escalable. Centrado en el cliente. Fiable y rentable.

Alcatel-Lucent OXO Connect es un sistema de telefonía escalable basado en una plataforma de comunicaciones robusta, conectada y convergente para empresas con hasta 300 usuarios. OXO Connect ofrece acceso integrado al servicio de colaboración basado en la nube Alcatel-Lucent Rainbow™.

Conjuntamente, OXO Connect y Rainbow ofrecen comunicaciones empresariales centradas en el cliente y servicios de colaboración de vídeo a todos los empleados, dondequiera que estén. Los profesionales de las Pymes trabajan mejor juntos para responder a las solicitudes de los clientes y pueden compartir la información con los invitados, clientes y business partners de una manera más rápida y precisa.

Disfrute de una gran fiabilidad con la tecnología de Alcatel-Lucent Enterprise, probada y validada del teléfono a la nube.

OXO Connect se ha optimizado para propiciar operaciones rentables: se ofrecen comunicaciones unificadas y gestión remota mediante conexión a un servicio de nube.

Funciones	Ventajas
Comunicaciones de nube híbrida escalables	Amplíe sus comunicaciones empresariales a medida que vaya creciendo, con usuarios adicionales y nuevos servicios de colaboración basados en la nube, entre los que figuran el servicio de número único para usuarios móviles o videoconferencias seguras.
Teléfonos empresariales avanzados y servicios de colaboración de nivel empresarial	Ofrezca una experiencia excepcional al cliente gracias a la mejora de la resolución en la primera llamada y la toma de decisiones: las llamadas se redirigen a los expertos adecuados y las reuniones virtuales permiten que la información fluya con mayor rapidez.
Conectividad híbrida para teléfonos y enlaces analógicos, digitales, IP y SIP	Aproveche la rápida amortización de la inversión al aprovechar la rentabilidad del cableado y teléfonos que requieren alimentación y mantenimiento mínimos. Reduzca los costes y aproveche las ventajas de una única red IP para voz y datos siempre que pueda.
Solución fiable que incluye LAN y WLAN, teléfonos y servidor de comunicaciones conectados a la nube	Proteja su inversión con una solución de Alcatel-Lucent Enterprise dedicada a las Pymes, 100% probada en laboratorio y validada de extremo a extremo del teléfono a la nube. La solución se actualiza desde la nube.

Datasheet
Alcatel-Lucent OXO Connect

OXO Connect Large 150W

OXO Connect Compact

OXO Connect Small

Servicios empresariales

Servicios de comunicaciones empresariales

Experiencia de comunicación

- Telefonía multilínea
- Búsqueda en directorios y llamada por nombre
- Buzón de voz visual y registro de llamadas
- Indicación de mensaje en espera
- Presencia
- Integración de telefonía e informática (CTI)
- Teléfonos con pantalla en color, táctil y personalizada
  - ¬ Navegación mediante pantalla táctil y teclado
  - ¬ Audio de alta calidad de banda super ancha y manos libres
  - ¬ Modelos de teléfono Bluetooth
  - ¬ Módulos adicionales
  - ¬ modulo wifi

Servicio de conversación

- Servicios de movilidad: modo Nomadic
  - ¬ Enrutamiento a varios dispositivos: teléfono empresarial, terminal DECT o WLAN, PC, smartphone
  - ¬ Servicio de número único
  - ¬ Reglas de enrutamiento definidas por el usuario
- Zona de escritorio/escritorio compartido
- Servicios de comunicaciones empresariales
  - ¬ Opción de llamadas, marcación rápida
  - ¬ Devolución de llamadas, colas de llamadas
  - ¬ Captura de llamadas, barge-in
  - ¬ Desvío de llamadas
  - ¬ Enrutamiento dinámico: sin respuesta, ocupada
  - ¬ Grabación de llamadas
  - ¬ Buscapersonas
  - ¬ DISA
- Equipo y grupo
  - ¬ Sistema de grupo de trabajo y clave
  - ¬ Supervisión de groupware
  - ¬ Notificaciones de audio
  - ¬ Grupo: modos de difusión, paralelo, cíclico y secuencial
  - ¬ Servicios Manager/Assistant (jefe/secretaria)
- Conferencia
  - ¬ Conferencia a tres
  - ¬ Conferencia a seis
  - ¬ Teléfonos de conferencia Alcatel-Lucent 8135s IP Conference Phone (5 tramos
  - ¬ Dispositivos de conferencia SIP (3 tramos)
- Número de emergencia
  - ¬ Número virtual: ubicación, PSAP
  - ¬ Servicio de notificación local

Teléfonos compatibles

- Analógico de 2 cables
  - ¬ Puertos analógicos
- Teléfonos empresariales de línea fija (protocolo NOE/IP)
  - ¬ ALE-DeskPhones Essential: ALE-20, ALE-20h, ALE-30, ALE-30h
  - ¬ ALE-DeskPhones Enterprise: ALE-300, ALE-400, ALE-500
  - ¬ Alcatel-Lucent 8088 V3 Smart DeskPhone
  - ¬ Alcatel-Lucent 8008G, 8008 DeskPhone
- Terminales empresariales móviles ¬ Alcatel-Lucent 8214 DECT, terminales: GAP
  - ¬ Alcatel-Lucent 8234, 8244, 8254, 8262, 8262EX DECT: Alcatel-Lucent AGAP
  - ¬ Alcatel-Lucent 8158s, 8168s WLAN
- Alcatel-Lucent IP Desktop Softphone: NOE/IP
  - ¬ Plataformas: Microsoft Windows, Android
- Teléfonos SIP
  - ¬ ALE-2, ALE-3 DeskPhones
  - ¬ Teléfonos Vtech para sectores hotelero y sanitario
- Alcatel-Lucent Rainbow: VoIP Softphone
- Módulos de conferencia
  - ¬ Teléfonos de conferencia Alcatel-Lucent 8135s IP Conference Phone
- Teléfonos de terceros (DSPP)
  - ¬ DECT (GAP), SIP (abierto y básico)

PIMphony

Servicios de telefonía y comunicaciones unificadas (CTI)

- Plataforma: Microsoft Windows (modo de escritorio)
- VoIP Softphone
- Supervisión multisitio
- Modo de asistente (operador)

Servicios de comunicaciones unificadas Rainbow

Servicio de nube híbrida entre teléfonos de OXO Connect y aplicaciones de Rainbow

- Servicios de comunicaciones unificadas
  - ¬ Gestión de contactos, presencia, uso compartido de calendarios, chat, llamada de audio/vídeo, uso compartido de pantalla y archivos
  - ¬ Chat de grupo permanente con prestaciones de conferencia con uso compartido de audio/vídeo/pantalla
  - ¬ Conferencias de audio de hasta 100 participantes
- Integración de nube híbrida con OXO Connect
  - ¬ Servicios de movilidad
  - ¬ CTI de teléfono empresarial: control de llamadas, buzón de voz visual, registro de llamadas, presencia de telefonía, llamadas de grupo, attendant
  - ¬ VoIP WebRTC sobre Internet: smartphone, PC, MAC, Web
- Servicios de autocuidado (para la administración de la empresa)
  - ¬ Servidor de llamadas Sincronización de directorio común con el directorio comercial Rainbow
  - ¬ Gestión de mensajes de voz de saludo
- Plataformas
  - ¬ Escritorio, Web, IOS, Android
  - ¬ Complemento de Microsoft Outlook, Active Directory de Microsoft Azure, Microsoft Teams

Servicios de bienvenida al cliente

ACD

Funciones integradas de OXO Connect

- Compatible con teléfonos empresariales Alcatel-Lucent, terminales DECT y WLAN, teléfonos SIP y dispositivos analógicos de otros fabricantes
- Las llamadas ACD y empresariales se pueden controlar simultáneamente en el teléfono empresarial
- Aplicaciones
  - ¬ Menús contextuales de agente desde el teléfono y la aplicación para PC
  - ¬ Aplicación en PC de supervisor para supervisión de actividades ACD en tiempo real de los agentes y puesta en cola de llamadas de grupo
  - ¬ Servicios de estadística con informes predefinidos
- Servicios
  - ¬ Selección de Grupo: tiempo máximo inactivo, rotación, prioridad, prioridad fija
  - ¬ Desbordamiento de grupo y niveles de prioridad entre grupos
  - ¬ Cola de grupo y guía de voz
  - ¬ Código de cliente
  - ¬ Pantalla emergente/CRM

Smart call routing SCR

Servicio que permite el enrutamiento de llamadas basado en diversos criterios

- Hasta 10.000 rutas
- Criterios de enrutamiento: código del cliente, CLI, DDI, planificación definida
- Destinos de enrutamiento: ACD, MLAA, cualquier destino

Saludo de bienvenida

- Asistente personal
- Servicios de operadora
  - ¬ Grupo de operadoras, cola de llamadas, desbordamiento de llamadas
  - ¬ Intervalo de tiempo: diario, semanas, festivos, control de modo restringido
  - ¬ Indicador de alarma
  - ¬ Gestión de PBX y usuarios finales
- Saludos
  - ¬ Saludos de la empresa
  - ¬ Saludos nocturnos
  - ¬ Música en espera
- Operadora automatizada (2 niveles)
- Operadora automatizada de varios idiomas (MLAA)
  - ¬ 5 árboles con 3 niveles por árbol
  - ¬ 5 idiomas por árbol
  - ¬ Intervalo de tiempo
- Bienvenida multiempresa: hasta 4 empresas

Servicios para mercados verticales

Sectores Hotelero y Sanitario

- Habitaciones de huéspedes y teléfonos administrativos: hasta 300 teléfonos
- Aplicación integrada: hasta 120 habitaciones
- Enlace Alcatel-Lucent OXO Connect Hospitality (OHL): hasta 300 habitaciones

Medición

- Contadores de medición y contadores de tráfico
- Enlace de tarificación
- Servicios de impresión
- Medición de llamadas local: XML/HTTP
- Código de cuenta
- Desconexión forzada basada en la duración
- Contabilidad de llamadas de base de duración (3 niveles)

Mensajería

- Buzón de voz: hasta 500 buzones de voz, 200 horas
- Mensajería instantánea (MI)
- Texto de mensajería (exclusivo de MI)
- Buzón de voz en correo electrónico
- Registro de llamadas en el correo electrónico

Servicios de directorio

- Marcación por nombre: modos automático y unificado
- Acceso a directorio universal: servidor LDAP/LDAPS externo
- Directorio integrado
- Directorios comunes y personales
- Directorios Rainbow

Aplicaciones e interfaces

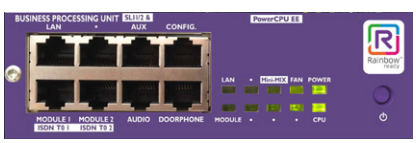
- Alcatel-Lucent OmniVista 8770 NMS: tarificación y recaudación de tickets VoIP, registro de detalles de llamadas
- Alcatel-Lucent Enterprise Application Partner Program (AAPP)
- QSIG
- Enlace SIP, Open SIP
- Rainbow CPaaS
- SNMP
- CSTA, TAPI 2.0, TAPI 2.1
- Alcatel-Lucent Hospitality
  - ¬ OLD: Office Link Driver
  - ¬ OHL: Hotel Link
- Tarificación de llamadas: servicios Web y OHL
- Aplicación de medición de llamadas local (LCMA)
- REST API para gestionar música en espera (MOH)
- Protección de trabajadores aislados (IWP)
  - ¬ Servidor de alarmas (enlace SIP, T2)

Conexión en red y topología

- Multisede
  - ¬ Hasta 5 sedes
  - ¬ Sincronización de directorios a través de la consola de administración
- Conexión en red
  - ¬ ISVPN (T0/T2)
  - ¬ QSIG-BC (DLT0 DLT2)
  - ¬ Enlaces SIP privados, varios enlaces SIP
  - ¬ Enlace SIP over Internet (SIP TLS SRTP con OCE Front End)
  - ¬ Selección automática de ruta (ARS): 3000 entradas, intervalo de tiempo, enrutamiento de menor coste
- Sucursal
  - ¬ Teléfono empresarial remoto: VPN IPSEC
  - ¬ Alcatel-Lucent 8378 IP DECT x-BS, estación base única Alcatel-Lucent 8328 SIP-DECT

Funcionamiento y mantenimiento

- OXO Management Console (OMC) en PC
- Rainbow Admin & Self-care (web)
- Alcatel-Lucent OmniVista 8770 NMS
- Alcatel-Lucent Cloud Connect, Fleet Dashboard de OXO Connect
- Servicios Plug and play sin intervención:
  - ¬ Servicios de comunicaciones unificadas Rainbow
  - ¬ Teléfonos empresariales y terminales móviles Alcatel-Lucent, estaciones (SUOTA) base DECT, OmniSwitch, OmniAccess Stellar, Rainbow WebRTC Gateway
  - ¬ Implantación de dispositivos de otros fabricantes
- Copia de seguridad/restauración: local, externa, MSDB
- Protocolo de hora de red (NTP), SNMP



Especificaciones técnicas

Arquitectura

Software

- Sistema operativo: Linux
- Paquete de software: Alcatel-Lucent OXO

Arquitectura del sistema

- Chasis "todo en uno"
- Enlace SIP TLS/SRTP con OCE Front End
- Conmutación IP híbrida e TDM
- Solución de communicaciones inificadas de nube hibrida
  - ¬ Agente Rainbow
  - ¬ Puerta de enlace Rainbow WebRTC Gateway
  - ¬ Aparato externo:
    Intel® NUC (max 50 canales)
    OCE Front End (max 20 canales)

Capacidad

- Máximo de usuarios (dispositivos): 300
- BHCA 1500

Conectividad

Conectividad

- IPv4
- HTTP/HTTPs
- VoIP
  - ¬ G.711, G.729, G.722, Super-Wide Band (OPUS), paso de códec (RTP directo)
  - ¬ QOS: TOS, DiffServ, 802.1 p/Q
  - ¬ RTP directo, proxy RTP, servidor de medios de software integrado
  - ¬ DTMF: en banda, RFC 2833
  - ¬ Normas IETF/ RFC
- FAX
  - ¬ Fax transparente G.711
  - ¬ T.38: solo RTP directo
- La puerta de enlace Rainbow WebRTC ofrece servicios de VOIP WebRTC por Internet
  - ¬ Reenvío de puertos compatible con cortafuegos y sin VPN
  - ¬ Medios cifrados, STUN/TURN
- Gestión: acceso remoto
  - ¬ Alcatel-Lucent Cloud Connect: HTTPS compatible con cortafuegos
  - ¬ IPsec con VPN integrada
  - ¬ RDSI (1 o 2B), devolución de llamada

SIP

- Enlace SIP público
- Enlace SIP privado
- Puntos finales SIP (usuarios locales)

Estaciones base DECT

- 8378 DECT IP-xBS: GAP y AGAP
- Estación base de celda única 8318 y 8328
  SIP-DECT: SIP y GAP
- 8379 DECT IBS, 8379 DECT IBS ATEX: GAP y AGAP

WLAN

- Puntos de acceso WLAN Alcatel-Lucent OmniAccess y controladores WLAN
- Alcatel-Lucent OmniAccess Serie Stellar AP

Seguridad

Autenticación

- Autenticación de usuarios
  - ¬ Contraseña de 6 dígitos
  - ¬ Acceso bloqueado después de errores de autenticación reiterados, notificación
  - ¬ Modos normal/restringido
  - ¬ Derecho del usuario a los servicios
  - ¬ PIN para acceso remoto (DISA)
- Certificado
  - ¬ Autofirmado de servidor
  - ¬ Importación para autoridad pública
- Acceso a WAN: compatible con proxy HTTP
- Autenticación SIP: RFC2617

Filtrado de tráfico

- Protección contra suplantación de direcciones ARP
- Defensa perimetral SIP
  - ¬ Cuarentena, lista negra, lista negra automatizada
  - ¬ Seguimiento de conexiones

Cifrado

- HTTPS (TLS 1.2)
- SIP TLS (TLS1.2) /SRTP (OCE Front End necesario)
  - ¬ Enlace SIP (privado/público)

Características físicas

Tarjeta de CPU de hardware

- PowerCPU EE (PowerPC e300)
  - ¬ Chasis: modelos Compacto, S, L 150w
  - ¬ 16 canales VoIP DSP (integrados)
  - ¬ Placa hija opcional VoIP 32: 48 canales VoIP
  - ¬ Placa hija opcional VoIP 64: 76 canales VoIP
  - ¬ Placa hija de almacenamiento de memoria (MSDB): 8 GB (eMMC)
- Placa hija (opcional)
  - ¬ AFU: reproductor de CD, portero automático, altavoz
  - ¬ HSL1 o HSL2: para interconexión de varios armarios (chasis S, L 150w)
  - ¬ MiniMIX 2/0/2 (solo chasis compacto)

Chasis

- Compact (C) Edition
  - ¬ Fuente de alimentación de CA/CC: externa
  - ¬ Batería auxiliar: externa (opcional)
  - ¬ Instalación: montaje en pared
  - ¬ 1 ranura modular libre
  - ¬ Sin ventilador
  - ¬ Altura: 70 mm (2,75 pulgadas)
  - ¬ Anchura: 345 mm (13,58 pulgadas)
  - ¬ Profundidad: 340 mm (13,38 pulgadas)
  - ¬ Peso (desembalado): 5,1 kg (11,24 lb)
  - ¬ Potencia máxima/estándar: 40 W/25 W
  - ¬ Nivel de ruido: 0 dBA
- Bastidores S, L 150w
  - ¬ Ventilador
  - ¬ Bastidor de 19 pulgadas
  - ¬ Fuente de alimentación de CA/CC: integrada
  - ¬ Batería auxiliar: interna/externa (opción)
  - ¬ Instalación: pila, bastidor, en pared
  - ¬ Combinación: hasta 3 chasis, máximo 27 ranuras libres
- Bastidor 1U pequeño (S)
  - ¬ 2 ranuras modulares libres
  - ¬ Altura: 66 mm (2,60 pulgadas)
  - ¬ Anchura: 442 mm (17,40 pulgadas)
  - ¬ Profundidad: 400 mm (15,75 pulgadas)
  - ¬ Peso (desembalado): 6 kg (13,22 lb)
  - ¬ Potencia máxima/estándar: 70 W/28 W
  - ¬ Nivel de ruido: máximo 40 dBA
- Bastidor 3U grande
  - ¬ 8 ranuras modulares libres
  - ¬ Altura: 154 mm (6,06 pulgadas)
  - ¬ Anchura: 442 mm (17,40 pulgadas)
  - ¬ Profundidad: 400 mm (15,75 pulgadas)
  - ¬ Peso (desembalado): 13 kg (28,7 lb)
  - ¬ Potencia máxima/estándar: 150W/75W
  - ¬ Nivel de ruido: 45 dBA máx.

Tarjetas de interfaz

- Terminales
  - ¬ Interfaces digitales UAI 8, 16
  - ¬ Interfaces analógicas SLI 8, 16

- Red
  - ¬ Tarjetas BRA: 4, 8 T0
  - ¬ Tarjetas PRA: 1 T1, T2
  - ¬ Enlace analógico: APA8
  - ¬ Tarjetas mixtas: T0/UA/SL 2/4/4, 4/4/8, 4/8/4
  - ¬ Tarjetas analógicas mixtas: APA/UA/SL 4/4/4-1, 4/4/8-1, 4/8/4-1
  - ¬ Mini-MIX2/0/2
- LAN
  - ¬ 10/100/1000 BT de detección automática no gestionada

Directivas internacionales

- CE y directivas de la UE
  - ¬ 1999/519/CE: SAR
  - ¬ 2009/125/CE: Diseño Eco
  - ¬ 2011/65/UE: ROHS
  - ¬ 2012/19/UE: WEEE
  - ¬ 2014/53/UE: RED
  - ¬ 2014/35/UE: LVD
  - ¬ 2014/30/UE: EMC
  - ¬ 2014/34/UE: ATEX
- Seguridad
  - ¬ IEC 60950-1
  - ¬ UL 60950-1
- SAR
  - ¬ Cenelec EN50360
  - ¬ Cenelec EN50385
  - ¬ Cenelec EN62311
  - ¬ FCC OET 65 e IEEE 1528
- EMC
  - ¬ IEC-CISPR22 Clase B
  - ¬ IEC-CISPR32 Clase B
  - ¬ Cenelec EN55022 Clase B
  - ¬ Cenelec EN55032 Clase B
  - ¬ FCC parte 15B
  - ¬ IEC-CISPR24
  - ¬ Cenelec EN55024
  - ¬ IEC-EN61000-3-2
  - ¬ ETSI-EN 301 489-06: DECT
  - ¬ ETSI-EN 301 489-17: Bluetooth y WLAN
- Radio
  - ¬ ETSI EN 300 328: 2,4 GHz
  - ¬ ETSI EN 301 893: 5 GHz
  - ¬ ETSI EN 301 406: DECT
  - ¬ FCC parte 15 subparte C, D, E
- Entorno EX
  - ¬ Cenelec EN 60079-0
  - ¬ Cenelec EN 60079-11
- Entornos variados
  - ¬ IEC 60945: marítima
- Condiciones ambientales
  - ¬ ETSI – ETS 300 019 parte 1-1: almacenamiento
  - ¬ ETSI – ETS 300 019 parte 1-2: transporte
  - ¬ ETSI – ETS 300 019 parte 1-3: en uso
- Telecomunicaciones
  - ¬ ETSI EG 201 121
  - ¬ ETSI ES 203 021
  - ¬ ETSI TBR 021, 010, 022, 003, 033, 004, 034, 008, 038
  - ¬ ITU-T H.323
  - ¬ FCC parte 68
  - ¬ Canadá CS03
- Exceso de tensión y de corriente
  - ¬ ITU-T K.21, K.22

Alcatel·Lucent Enterprise

VJNet

VCC TARIFICADOR

Todo bajo control

VCC Tarificador es una potente herramienta que permite administrar y mantener bajo control sus gastos telefónicos.

Consulte el detallado del tráfico telefónico al mismo tiempo que mide el desempeño de sus colaboradores, reduzca el mal uso del servicio telefónico, reciba notificaciones de llamadas no contestadas y mejore la calidad de su atención telefónica.

Tenga en todo momento la información clave de su empresa para la toma oportuna de decisiones.

Mucho mas que un tarificador de llamadas

Funciones principales

- Compatible con la marcación a 10 dígitos.
- Actualización de tablas de marcación a 10 dígitos sin costo extra.
- Reportes acumulados y por detalle, predefinidos y personalizables.
- Programación de envio de reportes automáticos a correo electrónico.
- Reportes imprimibles y con opción de exportarlos a Excel y a PDF.
- Estructura organizacional
    - Empresa
    - Sucursales
    - Departamentos
    - Áreas
    - Centro de costo
- Integración con MSAD.
- Widgets configurables mediante dashboard.
- Acceso a directorio institucional y marcación directa desde cualquier extensión con solo un click.
- Soporte de múltiples nodos
- Alta disponibilidad
- Reportes centralizados
- Resumen centralizado de trafico de llamadas entrantes y salientes.
- Asignación de saldo a extensiones, área, centro de costos mediante presupuesto, números de llamadas, minutos, duración etc.
- Cierre automático de llamadas por falta de saldo.
- Envió de correo electrónico de alerta en caso de haber terminado el saldo, cuando este a punto de ternarse o en llamadas no contestadas.
- Asignación automática de código de autorización con diferentes niveles de servicio y cierre automático al termino del saldo.
- Manejo de múltiples carriers.
- Múltiples tarifas según carrier y horario.
- Filtro de búsqueda
    - Top de mayor y menor uso
    - Trocal activa o inactiva.
    - Saturación de troncales.
    - Área.
    - Centro de costo.
    - Departamentos.
    - Tipo de Marcación (llamada interna, Fijo, celular, LDN, LDI, LDM).
    - Ubicación geográfica.
    - Fecha.
    - Hora.
    - Duración.
    - Número de teléfono.
    - Mayor o menor duración por extensión y por línea.
    - Canal.
    - Detalle de llamadas por extensión.
    - Grupo de extensiones.
    - Llamada interna/externa.
    - Entrante directa a DID o indirecta/saliente.
    - Llamadas sin contestar.
    - Por mayor o menor costo de llamada por extensión y por línea.
    - Gasto telefónico.
    - Código de autorización.

Base de datos internas

- MS-SQL Server.
- MS-SQL Express.
- MySQL.
- Almacenamiento mínimo de 1 año para tickets (depende de tamaño de disco duro)

Administración

- Administración y supervisión grafica, GUI y WEB.
- Software Intuitivo y multisesión.
- Multiples niveles de servicio.
- Envio de alarmas en tiempo real por correo electrónico, traps SNMP y SMS.
- Umbral de alarmas configurables.
- Comunicación cifrada cliente-servidor.
- Funcionamiento en LAN y WAN.

Integración/compatibilidad

- Fácil integración con cualquier CRM vía REST API.
- Desarrollos especiales a medida.
- Conexión IP con respuesta de Eco.
- Consumo de archivo directo.
- IP.
- SMDR.
- Telnet.
- SSH.
- RS232.
- WEB Services.
- CTI.
- CSTA.
- TAPI.
- Alcatel-Lucent
    - OmniPCX Office
    - OmniPCX Enterprise
- CISCO
    - CallManager
    - CallManager Express.
- AVAYA
- Asterisk
- Panasonic
- Grandstream
- VCC Voice

Especificaciones técnicas

ON-PREMISE y CLOUD
Alta disponibilidad
Windows server 2016, 2019 y 2022.
Windows 10 Pro y 11.
Virtualizable

- VMWare
- KVM
- Virtual Box

físico o virtual: Quad Core CPU, 8MB L2 cache, 8 GB RAM.

Mensajes de texto SMS

- Envio de mensajes informativos de llamadas realizadas a números no autorizados.
- Aviso de termino o próximo termino de saldo en extensión especifica o por grupos.
- Aviso de llamadas sin contestar en extensiones especificas o en todo el sistema.
- Mediante el envió de mensajes de texto SMS se puede realizar la solicitud de reporte de llamadas y recibirlo a un correo electrónico preconfigurado.

*(Requiere modulo VCC SMS)

Seguridad

- Cifrado de base de datos.
- Cifrado en la comunicación cliente-servidor.
- Registro de todos los movimientos realizados por los usuarios.
- Cuatro perfiles definidos por default
    - Agente
    - Supervisor
    - Operadora
    - Super usuario

Monitor de calidad

- Identificación de llamadas mediante a banderillas de colores
- Múltiples listas de reproducción según tipo de llamada. Una llamada importante, puede enviarse a una lista especifica para su fácil identificación y para generar reportes específicos.

Hardware

- Escalable.
- Alta disponibilidad
- Centralización de multisitios.
- Virtualizable
    - VMWare
    - KVM
    - Virtual Box

IVR

- Es posible acceder al directorio telefónico institucional configurado en el tarificador, mediante llamada telefónica de cualquier extensión de su conmutador y dictar el nombre de la persona a la que se quiera llamar, puede escuchar su número de extensión y llamar después o llamar en ese momento directamente. (requiere Google ASR).
- Escuchar la lista, consultar, agregar y eliminar números telefónicos de la lista negra.
- Escuchar saldos y movimientos de llamadas, por extensión o grupo de extensiones, mediante text to speech (TTS).
- Sin necesidad de acceder a una aplicación en su computadora, es posible llamar desde cualquier extensión de su conmutador y solicitar el envió de reportes de llamadas y recibirlo al correo electrónico.

*(Requiere modulo VCC IVR)

Grabación de llamadas

- No solo se conforme con tener información en texto de sus llamadas telefónicas, gracias al modulo VCC Recorder, ahora también es posible guardar el audio de todas las llamadas de su empresa.

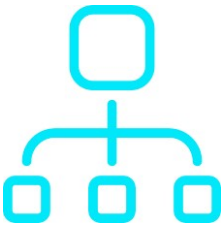
*(Requiere modulo VCC Recorder)

Multisitio

Puede gestionar al mismo tiempo, varios conmutadores ubicados en diferentes sucursales y de esta manera centralizar y facilitar la administración de los reportes.

Reportes acumulados y por detalle

Cuenta con una gran variedad de reportes predefinidos, por detalle de llamada o por acumulado y brinda las herramientas necesarias para generar reportes personalizados.



Estructura organizacional

Facilita la asignación de recursos y el control de reportes, mediante la estructuración de la organización dividida en: empresa, sucursales, departamentos, áreas, código de usuario y usuarios.

Centro de costos

Pude asignar saldo a cada sucursal, departamento, área o extensión especifica y en caso de excederlo, el sistema envía un correo informando al supervisor.

Múltiples tarifas y carriers

Es posible manejar diferentes costos en las tarifas de las llamadas telefónicas, dependiendo del proveedor por donde se realice la comunicación o bien la hora del día.

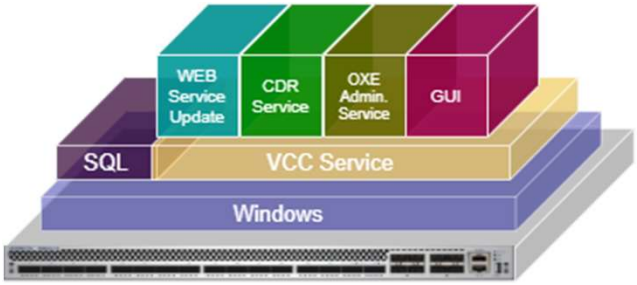
Envió de reportes y alarmas

Puede programar envió automático mediante correo electrónico y mensajes SMS, de reportes personalizados, acumulados o por detalle, así como alarma del sistema.

Diagrama de funcionamiento

- Conexión IP con respuesta de Eco.
- Consumo de archivo directo.
- IP.
- SMDR.
- Telnet.
- SSH.
- RS232.
- WEB Services.
- CTI.
- CSTA.
- TAPI.

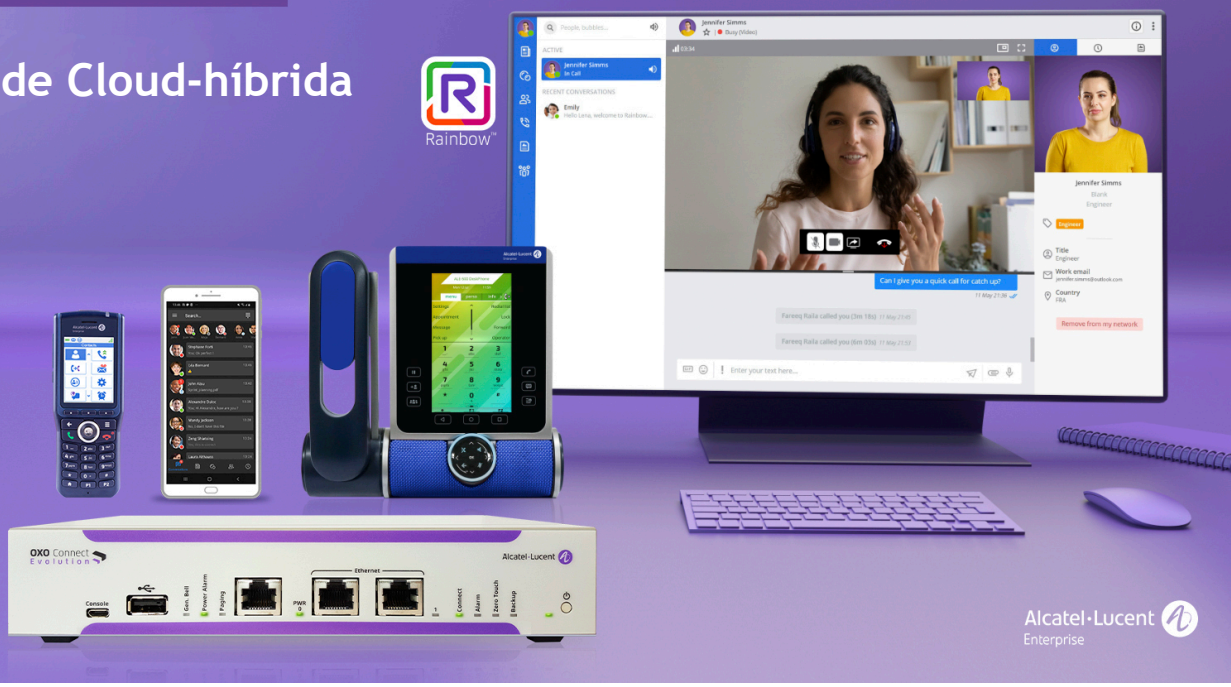
Estructura del software



FOLIO. 61

OXO CONNECT

Plataforma de Cloud-híbrida para PYMES



OXO Connect Evolution

Documentación especializada de: seguridad

Versión 6.1 - Abril 2024

8AL91230ESAI Ed.1

Alcatel·Lucent Enterprise

Aviso legal

El nombre y el logotipo Alcatel-Lucent son marcas registradas de Nokia que se usan bajo licencia por ALE. Para saber de otras marcas utilizadas por las empresas filiales de ALE holding, visite: www.al-enterprise.com/es-es/legal/marcas-comerciales-copyright. Todas las demás marcas comerciales son propiedad de sus respectivos propietarios.

La información incluida puede modificarse sin previo aviso. ALE Holding no asume ninguna responsabilidad por las posibles inexactitudes del contenido.

www.al-enterprise.com/es-es

Renuncia

A pesar de que se han realizado todos los esfuerzos necesarios para verificar la integridad y la precisión de la información que aquí se incluye, este documento se presenta "tal y como está". Para obtener información más precisa acerca de las compatibilidades cruzadas, los límites del producto, la política sobre el software y las listas de funciones, consulte los documentos exactos publicados en el sitio web del Business Partner: https://myportal.al-enterprise.com.

A fin de mantener un desarrollo continuado del producto, ALE International se reserva el derecho de realizar mejoras en esta documentación y en los productos que en ella se describen en cualquier momento y sin que tenga la obligación de realizar ningún aviso previo.

La marca CE indica que este producto cumple las Directivas comunitarias siguientes:

- 2014/53/EU para equipo de radio
- 2014/35/EU y 2014/30/EU para equipos que no sean de radio (incluido equipo terminal por cable)
- 2014/34/EU para equipo ATEX
- 2011/65/UE (RoHS)
- 2012/19/UE (RAEE)

CE

Sumario

Documentación especializada de: seguridad

Sumario

Documentación especializada de: seguridad

Capítulo 1

Estructura de la documentación especializada

La documentación especializada de OXO Connect Evolution se divide en quince documentos independientes. Además, el documento de Compatibilidad cruzada es la referencia donde consultar el estado detallado de dispositivos y aplicaciones compatibles e incompatibles.

Tabla 1-1 Estructura de la documentación especializada

	Título de la documentación	Número de pieza
[1]	Documentación especializada: presentación general Este documento contiene información general sobre OXO Connect Evolution. Aquí hallará, entre otras cosas, una breve descripción de los servicios que se ofrecen, el hardware de la plataforma, los teléfonos y aplicaciones de usuario disponibles, los límites, el cumplimiento con las normativas y las restricciones del entorno.	8AL91218ESAI
[2]	Documentación especializada: hardware (plataforma, interfaces y dispositivos) Este documento engloba todos los aspectos de hardware relacionados con OXO Connect Evolution. También contiene los procedimientos de puesta en servicio de los terminales.	8AL91219ESAI
[3]	Documentación especializada: servicios para el usuario Este documento muestra la presentación y el procedimiento de configuración de las funciones disponibles para los usuarios finales. En el último capítulo del documento, se resumen las funciones disponibles según el tipo de dispositivo o aplicación.	8AL91220ESAI
[4]	Documentación especializada: buzón de voz En este documento, se describen el sistema de buzón de voz integrado y la operadora automática (descripción general, gestión y servicios disponibles para usuarios finales), además del procedimiento de configuración para conectar una unidad de buzón de voz externa.	8AL91221ESAI
[5]	Documentación especializada: movilidad Este documento contiene una descripción detallada de los servicios de movilidad disponibles en OXO Connect Evolution. Incluye información de utilidad para ejecutar una infraestructura xBS, una descripción de las estaciones de base y teléfonos asociados. **Nota:** En este documento, no se describe la tecnología VoWLAN.	8AL91222ESAI
[6]	Documentación especializada: servicios VoIP En este documento, se describen los protocolos VoIP que admite OXO Connect Evolution (como SIP), el procedimiento de configuración del acceso público o privado a través de enlaces IP y la información básica sobre dimensiones y mantenimiento.	8AL91223ESAI

Capítulo 1 *Estructura de la documentación especializada*

	Título de la documentación	Número de pieza
[7]	Documentación especializada: redes privadas	8AL91224ESAI
[8]	Documentación especializada: aplicaciones generales Este documento ofrece una descripción de diversas aplicaciones disponibles en OXO Connect Evolution, como Hotel, Tarificación de llamadas, CTI, Centro de gestión de redes, Operadora automática múltiple. Entidades múltiples, PIMphony.	8AL91225ESAI
[9]	Documentación especializada: Web-Based Tool En este documento, se describe la Web-Based Tool, que es la herramienta de supervisión integrada de OXO Connect Evolution.	8AL91226ESAI
[10]	Expert Documentation: OmniTouch Call Center Office Este documento proporciona la descripción y el procedimiento de instalación de OmniTouch Call Center Office. Incluye también la presentación y el funcionamiento de las aplicaciones Announcement y Traceability, así como una breve descripción de las aplicaciones Agent, Statistics y Supervisor.	8AL91227ESAI
[11]	Documentación especializada: herramientas de gestión En este documento, se describe la herramienta de gestión disponible para OXO Connect Evolution (OMC). El documento describe el procedimiento de instalación de OMC, los distintos tipos de acceso entre OMC y OXO Connect Evolution (local, remoto, con o sin proxy), el procedimiento de instalación del software de OXO Connect Evolution a través de OMC y la lista de servicios que pueden gestionarse con OMC.	8AL91228ESAI
[12]	Documentación especializada: servicios de mantenimiento Este documento contiene información básica relativa al mantenimiento de OXO Connect Evolution. Incluye la metodología de diagnóstico en caso de avería de los terminales del sistema, la lista de mensajes del sistema, el procedimiento para guardar/restaurar datos, el procedimiento para detener/reiniciar el sistema y el modo de sustituir los terminales.	8AL91229ESAI
[13]	Documentación especializada de: seguridad Este documento proporciona información esencial para proteger OXO Connect Evolution. Incluye una guía de implantación de certificados, gestión de contraseñas, gestión de acceso a servicios desde redes LAN/WAN y configuración de red para acceso remoto.	8AL91230ESAI
[14]	Documentación especializada: servicios del sistema Este documento proporciona información sobre las claves de software e incluye una lista completa de ellas. El documento describe además el funcionamiento de OXO Connect Evolution con NTP (como cliente o servidor) y la configuración del servidor DHCP integrado.	8AL91231ESAI
[15]	Glosario Este documento contiene un glosario de términos generales empleados en telecomunicaciones, así como de términos específicos relacionados con OXO Connect Evolution.	8AL91232ESAI
[16]	Server Deployment Guide for Remote Workers using DeskPhones	8AL90345ENAA

Capítulo 1 *Estructura de la documentación especializada*

En el presente documento, las referencias a otros documentos se indican mediante el número en la primera columna de la tabla anterior.

Los números de pieza se indican en la última columna.

Capítulo 2

Visualización de parámetros del sistema

Los parámetros del sistema pueden encontrarse en archivos del sistema de archivos del OXO Connect Evolution.

Ofrece fácil acceso:

- Se puede acceder a los parámetros del sistema desde la página de inicio del OXO Connect Evolution
- La ID de la CPU puede mostrarse en los terminales 8058s Premium DeskPhone, 8068s Premium DeskPhone y 8078s Premium DeskPhone.

Para mostrar los parámetros del sistema desde la página de inicio del OXO Connect Evolution:

1. Conéctese a http://<nombre o dirección IP de OXO Connect Evolution> o https://<nombre o dirección IP de OXO Connect Evolution><:puerto>.

   Importante:

   Es muy importante aplicar medidas de seguridad adecuadas en la configuración del enrutador de acceso/cortafuegos para activar el acceso remoto al servidor de OXO Connect Evolution.

   El acceso remoto se debe activar únicamente si es necesario.

   Si se necesita activar el acceso remoto, deben ponerse en práctica las recomendaciones incluidas en la sección Seguridad - Configuración de la red para acceso remoto *(en la página 84)*.

   Aparecerá la página de inicio de OXO Connect Evolution.

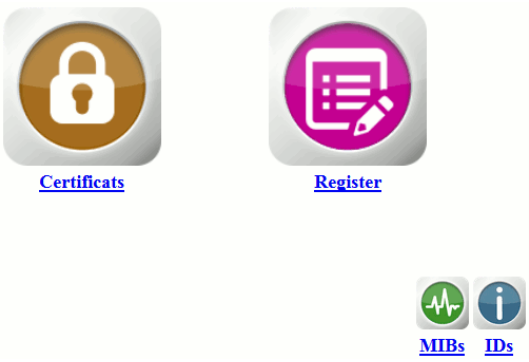


Figura 2-1 Página de inicio de OXO Connect Evolution

2. Haga clic en el enlace **IDs**

Capítulo 2 *Visualización de parámetros del sistema*

Se muestra la página de parámetros del sistema.

SERIAL	FFD04B91
ETH ADDR	00:80:9F:9D:37:C6
ID	[001:008a0c39]

Los parámetros del sistema mostrados son:

- Serial number
- Dirección MAC Ethernet de la CPU
- Identificador del fabricante del sistema (banda Proftp)

Para mostrar la ID de la CPU en un teléfono 8058s Premium DeskPhone, 8068s Premium DeskPhone y 8078s Premium DeskPhone, seleccione **Sistema** > **ID de la CPU** en la página **Menú**.

Capítulo 3

Cifrado nativo

3.1. Descripción general del cifrado nativo

El **cifrado nativo** proporciona capacidades de cifrado de bajo coste y fáciles de implementar a las PBX de OXO Connect Evolution que se ejecutan en las instalaciones del cliente.

Por defecto, **el cifrado nativo** viene habilitado y funciona sin configuración Para más información sobre el nivel de servicio disponible «listo para usar», consulte Cifrado nativo genérico (solución lista para usar) *(en la página 14)*.

La solución **Cifrado nativo** ofrece:

- Cifrado Datagram Transport Layer Security (DTLS) de los flujos de señalización intercambiados entre OXO Connect Evolution y los siguientes dispositivos IP compatibles con DTLS:
  - Teléfonos de oficina IP (8008/8008G/8018 DeskPhones, teléfonos premium 8028s/8058s/8068s/8078s, ALE-20/20h/30/30h Essential DeskPhone, ALE-300/400/500 Enterprise DeskPhone y 8088 Smart DeskPhone)

    En los teléfonos de oficina IP compatibles con DTLS, se muestra un icono de una llave en la parte superior de la pantalla cuando el enlace de señalización con OXO Connect Evolution se ha cifrado.
  - IP Desktop SoftPhones
  - Servidores VPN IPsec

    Esto se aplica a los teléfonos de trabajadores remotos conectados a la LAN de la empresa a través de una conexión VPN que se ha establecido mediante un servidor VPN IPsec. DTLS debe configurarse en el servidor VPN IPsec. Para obtener más información, consulte el documento [16].
- Autenticación del servidor o los extremos (servidor y dispositivos IP compatibles con DTLS) al establecer la conexión DTLS

La solución de **cifrado nativo** no ofrece:

- Cifrado de flujos de medios (voz): los flujos de medios emplean el protocolo RTP
- Cifrado de la transmisión DTMF para llamadas a través de enlaces SIP: los dígitos DTMF se envían en abierto mediante el protocolo RTP

Capítulo 3 Cifrado nativo

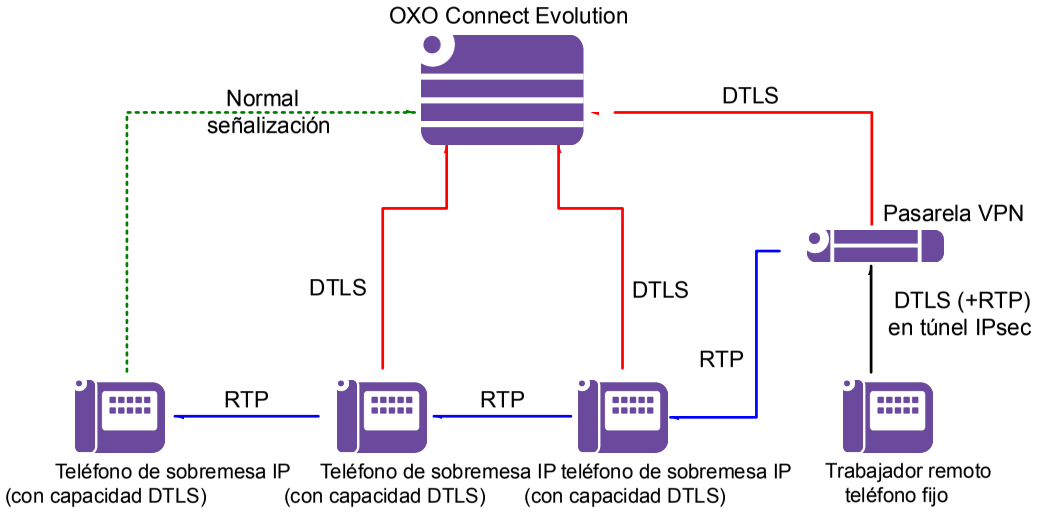


Figura 3-1 Ejemplo de vista de la solución de **cifrado nativo**

3.2. Autenticación y certificados de cifrado nativo

3.2.1. Autenticación del servidor y el cliente para las conexiones DTLS

El protocolo DTLS es compatible con dos métodos de autenticación:

- **Autenticación del servidor** (habilitada por defecto): en la negociación de la sesión de DTLS, OXO Connect Evolution (PBX) envía el certificado al cliente (dispositivo IP compatible con DTLS). El cliente autentica la PBX al verificar el certificado, usando la PBX CTL presente en el almacenamiento de confianza. La PBX CTL debe implementarse en el almacenamiento de confianza del cliente, ya sea de forma manual o a través del mecanismo **Aprovisionamiento automático de la TrustList de extremos** (consulte Implementación de listas de confianza de certificados (CTL) en dispositivos IP *(en la página 12)*). La PBX no solicita el certificado del cliente y no autentica a este último (dispositivo IP compatible con DTLS).
- **Autenticación de extremos**: en la conexión a una sesión DTLS, el servidor envía su propio certificado y solicita el certificado del cliente. Cuando el cliente ha autenticado el certificado del servidor, devuelve su propio certificado. El servidor autentica el certificado del cliente de vuelta. Para habilitar la autenticación de extremos, consulte Activar/desactivar la autenticación de los extremos *(en la página 22)*.

Capítulo 3 Cifrado nativo

3.2.2. Autenticación de servidor mediante certificados

Los certificados implementados en OXO Connect Evolution pueden ser:

- Certificados internos generados automáticamente y firmados por la autoridad de certificación de Alcatel-Lucent Enterprise.

  Por defecto, todas las PBX incluyen la misma autoridad de certificación genérica de Alcatel-Lucent Enterprise y pares de claves correspondientes. Durante la instalación, cada PBX genera automáticamente su propio certificado de servidor a partir de esta autoridad de certificación genérica. El certificado de servidor se genera con la dirección IP de la PBX como nombre destacado. La autoridad de certificación genérica no puede eliminarse en la PBX.

  Por defecto, la autoridad de certificación se encuentra en **modo estándar** cuando se inicia y el **cifrado nativo** está activado en la configuración de la PBX. En el **modo estándar**, la PBX utiliza un certificado interno generado automáticamente para su autenticación en la conexión DTLS. Esto se aplica a Cifrado nativo genérico (solución lista para usar) *(en la página 14)*.

- Certificados firmados por autoridades de certificación que no son de Alcatel-Lucent Enterprise (en lo siguiente, «certificados específicos»).

  Los certificados específicos los genera una PKI externa. La PBX permite generar una solicitud de firma de certificado local a través de la Web-Based Tool. Esta debe enviarse a la PKI externa para obtener un certificado de servidor específico firmado por una autoridad de certificación que no sea de Alcatel-Lucent Enterprise.

  El certificado específico y su autoridad de certificación deben importarse en la PBX. Tras importar y reiniciar la PBX, esta cambia al **modo experto** y usa este certificado específico para la autenticación en la conexión DTLS. Esto se aplica al **cifrado nativo** con seguridad total o forzada (consulte Cifrado nativo con seguridad total *(en la página 15)* o Cifrado nativo con seguridad forzada *(en la página 16)*).

  Si se deben generar certificados específicos para dispositivos IP compatibles con DTLS, la PKI externa debe proporcionar certificados para los dispositivos IP compatibles con PBX y DTLS firmados por la misma autoridad de certificación distinta de Alcatel-Lucent Enterprise.

  La autoridad de certificación que no sea deAlcatel-Lucent Enterprise y los archivos de certificado de servidor específicos deben estar en formato PKCS#12 o PKCS#7 e importarse a la PBX a través de la Web-Based Tool (véase: Configurar los certificados en la PBX *(en la página 24)*). Una vez que el certificado específico se importa en la PBX, reemplaza el certificado interno generado automáticamente y la PBX debe reiniciarse para tener en cuenta el certificado específico.

  Si los certificados específicos importados en dos PBX se han generado en la misma autoridad de certificación que no sea de Alcatel-Lucent Enterprise los dispositivos IP compatibles con DTLS pueden moverse de una PBX a la otra sin desactivar el **cifrado nativo**.

  Si se generan certificados específicos para dispositivos IP compatibles con DTLS, se deben importar manualmente en los dispositivos IP compatibles con DTLS a través de la MMI local. Estos certificados específicos reemplazan el certificado predeterminado de Alcatel-Lucent Enterprise generado durante el proceso de fabricación del dispositivo IP.

3.2.3. Implementación de listas de confianza de certificados (CTL) en dispositivos IP

Se configura una lista de confianza de certificados (CTL) en la PBX Esta CTL incluye el certificado de la CA que ha emitido el certificado de servidor (consulte). Esta CTL incluye el certificado de la CA que ha emitido el certificado de servidor (consulte Autenticación de servidor mediante certificados *(en la página 12)*).

Capítulo 3 *Cifrado nativo*

Para permitir que los dispositivos IP autentiquen el servidor durante las conexiones DTLS, la CTL debe implementarse en el almacenamiento de confianza de los dispositivos IP. Hay dos maneras de hacer esto:

- **Adquisición automática de CTL**: los dispositivos IP recuperan la CTL mediante el archivo `lanpbx.cfg` descargado de la PBX. La primera adquisición de la CTL se lleva a cabo en el modo **Aprovisionamiento automático de la TrustList de extremos**. Permite que un dispositivo IP en estado de fábrica (o un dispositivo IP con un almacenamiento de confianza vacío) establezca su primera conexión DTLS sin comprobar el certificado del servidor. Si el enlace de señalización se ha establecido correctamente, la CTL recibida mediante el archivo `lanpbx.cfg` se almacena en el almacenamiento de confianza del dispositivo IP. Las siguientes conexiones DTLS a la PBX se autentican por completo mediante la CTL almacenada. Con el modo **Aprovisionamiento automático de la TrustList de extremos**, la primera conexión DTLS será la única que se lleve a cabo sin una autenticación real.

  El dispositivo IP comprueba la integridad del archivo `lanpbx.cfg` cada una de las veces, siempre que el **cifrado nativo** esté activado. Durante la negociación TFTP inicial, la PBX envía el archivo `lanpbx.cfg` al dispositivo IP. El dispositivo IP comprueba la integridad del archivo `lanpbx.cfg` mediante la verificación de la firma del certificado de servidor. Tanto el certificado de servidor como la firma están integrados en el archivo `lanpbx.cfg`.
- **Adquisición manual de la CTL**: los dispositivos IP deben aprovisionarse individualmente con la CTL antes de conectarse a la PBX. Esta operación es posible mediante la importación manual de un archivo PEM en el dispositivo IP a través de MMI local, o bien mediante el mecanismo del protocolo simple de inscripción de certificados (SCEP): los dispositivos IP inician un proceso de inscripción SCEP para actualizar su CTL.

  La adquisición manual de la CTL aborda el **cifrado nativo** con total seguridad, donde los certificados para la PBX y los dispositivos IP se han generado a partir de una PKI externa y los certificados deben implementarse manualmente en teléfonos IP (consulte Cifrado nativo con seguridad total *(en la página 15)*).

La selección entre ambos métodos se define en el parámetro **Aprovisionamiento automático de la TrustList de extremos**, en la configuración de la PBX (consulte Habilitar/deshabilitar la implementación automática de la CTL (Aprovisionamiento automático de la TrustList de extremos) *(en la página 21)*):

- Si la PBX está en modo **estándar**, la **adquisición automática de la CTL** se habilita en la PBX y no se podrá modificar.
- Si la PBX está en modo **experto**, la **adquisición automática de la CTL** se habilita en la PBX (valor predeterminado) y se podrá modificar. Si la **adquisición automática de la CTL** está deshabilitada, la CTL no se incluirá en el archivo `lanpbx.cfg` cargado por los dispositivos IP.

Cuando se produce un cambio de CA desde una PKI externa, la PBX se reinicia para tener en cuenta el cambio: la CTL, incluida la nueva CA, se agrega al archivo `lanpbx.cfg`. Debe reiniciar los dispositivos IP para actualizar su almacenamiento de confianza con la nueva CTL recuperada a través del archivo `lanpbx.cfg`, descargado desde la PBX.

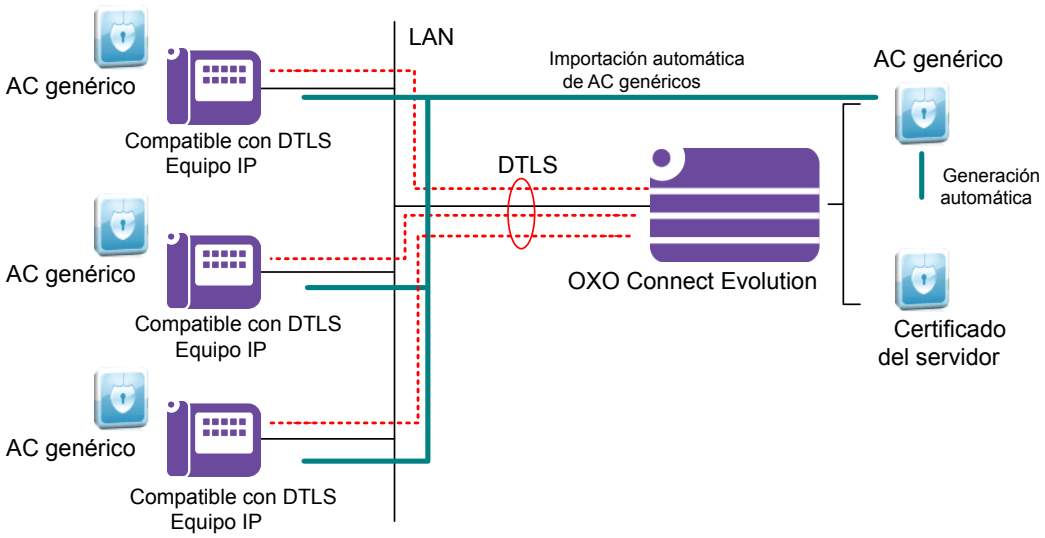
Capítulo 3 Cifrado nativo

3.3. Niveles de seguridad del cifrado nativo

3.3.1. Cifrado nativo genérico (solución lista para usar)

Cuando la PBX (OXO Connect Evolution) se implementa en las instalaciones del cliente, el **cifrado nativo** se activa automáticamente y las conexiones entre la PBX y los dispositivos IP compatibles con DTLS se establecen automáticamente con DTLS. Por defecto, la PBX está en modo **estándar** y el **cifrado nativo** no requiere ninguna configuración adicional en la PBX.

Este primer nivel de seguridad proporciona unas conexiones seguras y sólidas a través de DTLS, combinadas con una política de autenticación básica.



Durante la instalación, la PBX genera automáticamente su propio certificado de servidor a partir de la autoridad de certificación genérica de Alcatel-Lucent Enterprise. Añade la CA genérica a una lista de confianza de certificados (CTL) e incluye esta lista en el archivo `lanpbx.cfg`.

Los dispositivos IP compatibles con DTLS recuperan automáticamente la CTL (incluida la CA genérica) a través del mecanismo **Aprovisionamiento automático de la TrustList de extremos** (consulte Implementación de listas de confianza de certificados (CTL) en dispositivos IP *(en la página 12)*). La CTL se almacena en el almacenamiento de confianza de cada dispositivo IP compatible con DTLS.

En la negociación de la sesión DTLS, los dispositivos IP compatibles con DTLS autentican el certificado de servidor enviado por la PBX con la CTL almacenada en su almacenamiento de confianza. Tras la autenticación, los dispositivos IP compatibles con DTLS establecen una conexión DTLS segura con la PBX a través de la LAN.

Los dispositivos IP compatibles con DTLS se pueden mover de esta PBX segura a otra PBX, siempre que cumplan con las reglas descritas: Mover dispositivos IP de una PBX a otra *(en la página 25)*.

Capítulo 3 Cifrado nativo

3.3.2. Cifrado nativo con seguridad total

La PBX puede implementarse en instalaciones de clientes que necesiten un alto nivel de seguridad, en las que:

- Se use una PKI externa para generar certificados de servidor específicos a partir de una autoridad de certificación que no sea deAlcatel-Lucent Enterprise para todos los dispositivos conectados a la red del cliente
- La autoridad de certificación que no sea de Alcatel-Lucent Enterprise y los certificados específicos se importan manualmente en la PBX y los dispositivos IP

Este elevado nivel de seguridad proporciona unas conexiones seguras y sólidas a través de DTLS, combinadas con una política de autenticación sólida.

En este entorno tan seguro, el **cifrado nativo** debe configurarse de la siguiente manera:

- La autoridad de certificación que no sea de Alcatel-Lucent Enterprise y el certificado específico deben importarse a la PBX a través de la Web-Based Tool (véase: Configurar los certificados en la PBX *(en la página 24)*)

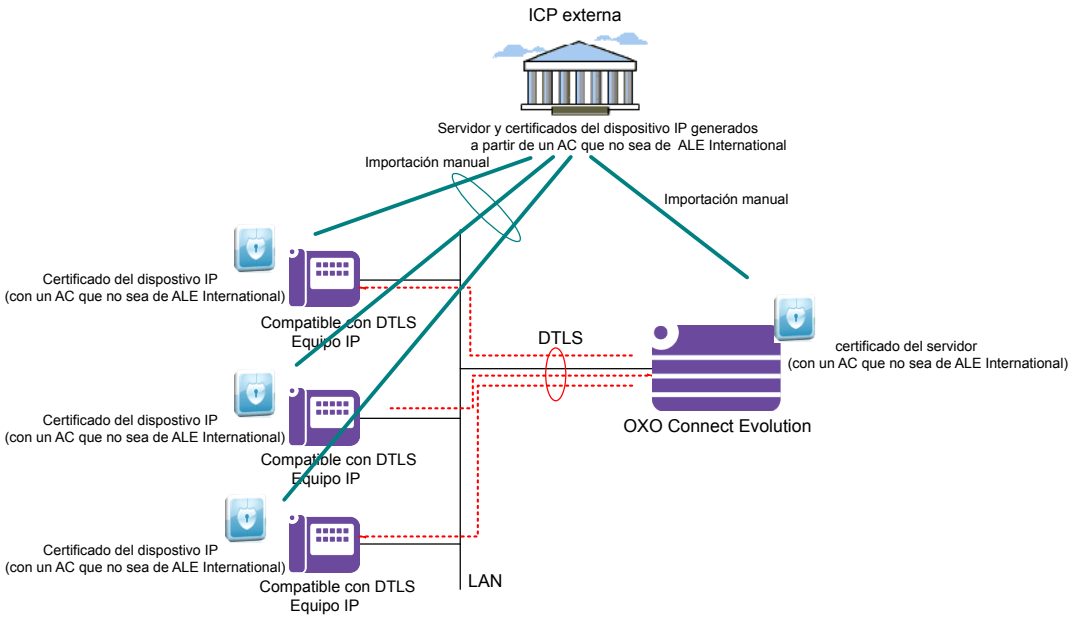
  Tras importar y reiniciar la PBX, esta cambia al **modo experto** y el **cifrado nativo** se activa automáticamente en la PBX. En el **modo experto**, la PBX usa este certificado específico para la autenticación en la conexión DTLS.
- La autoridad de certificación que no sea de Alcatel-Lucent Enterprise y el certificado específico deben importarse en la CTL de cada dispositivo IP compatible con DTLS mediante una MMI local
- El parámetro **Aprovisionamiento automático de la TrustList de extremos** debe deshabilitarse en la PBX mediante la aplicación **OMC** (consulte Habilitar/deshabilitar la implementación automática de la CTL (Aprovisionamiento automático de la TrustList de extremos) *(en la página 21)*)

  Esta operación evita cualquier descarga automática de CTL de PBX en el almacenamiento de confianza de dispositivos IP compatibles con DTLS
- El parámetro **Autenticación de extremos** debe deshabilitarse en la PBX mediante la aplicación **OMC** (consulte Activar/desactivar la autenticación de los extremos *(en la página 22)*)

Además, solo los dispositivos IP compatibles con DTLS pueden conectarse a la PBX. Por defecto, en el modo **experto**, el parámetro **Modo DTLS forzado** está habilitado en la PBX (consulte Activar/desactivar el modo DTLS forzada *(en la página 23)*)

Capítulo 3 *Cifrado nativo*

En la negociación de la sesión DTLS, los dispositivos IP compatibles con DTLS autentican el certificado de servidor con la autoridad de certificación que no sea de Alcatel-Lucent Enterprise almacenada en su almacenamiento de confianza. Tras la autenticación, los dispositivos IP compatibles con DTLS establecen una conexión DTLS segura con la PBX a través de la LAN.



Los dispositivos IP compatibles con DTLS se pueden mover de esta PBX segura a otra PBX, siempre que cumplan con las reglas descritas: Mover dispositivos IP de una PBX a otra *(en la página 25)*.

3.3.3. Cifrado nativo con seguridad forzada

La PBX puede implementarse en instalaciones de clientes que necesiten un alto nivel de seguridad, en las que:

- Se use una PKI externa para generar certificados de servidor específicos a partir de una autoridad de certificación que no sea deAlcatel-Lucent Enterprise para todos los dispositivos conectados a la red del cliente
- Los dispositivos IP compatibles con DTLS recuperan la CTL (incluida la CA que no sea de Alcatel-Lucent Enterprise) a través del mecanismo **Aprovisionamiento automático de la TrustList de extremos** (consulte Implementación de listas de confianza de certificados (CTL) en dispositivos IP *(en la página 12)*).

Capítulo 3 Cifrado nativo

En este entorno tan seguro, el **cifrado nativo** debe configurarse de la siguiente manera:

- La autoridad de certificación que no sea de Alcatel-Lucent Enterprise y el certificado específico deben importarse a la PBX a través de la Web-Based Tool (véase: Configurar los certificados en la PBX *(en la página 24)*)

  Tras importar y reiniciar la PBX, esta cambia al **modo experto** y el **cifrado nativo** se activa automáticamente en la PBX. En el **modo experto**, la PBX usa este certificado específico para la autenticación en la conexión DTLS.

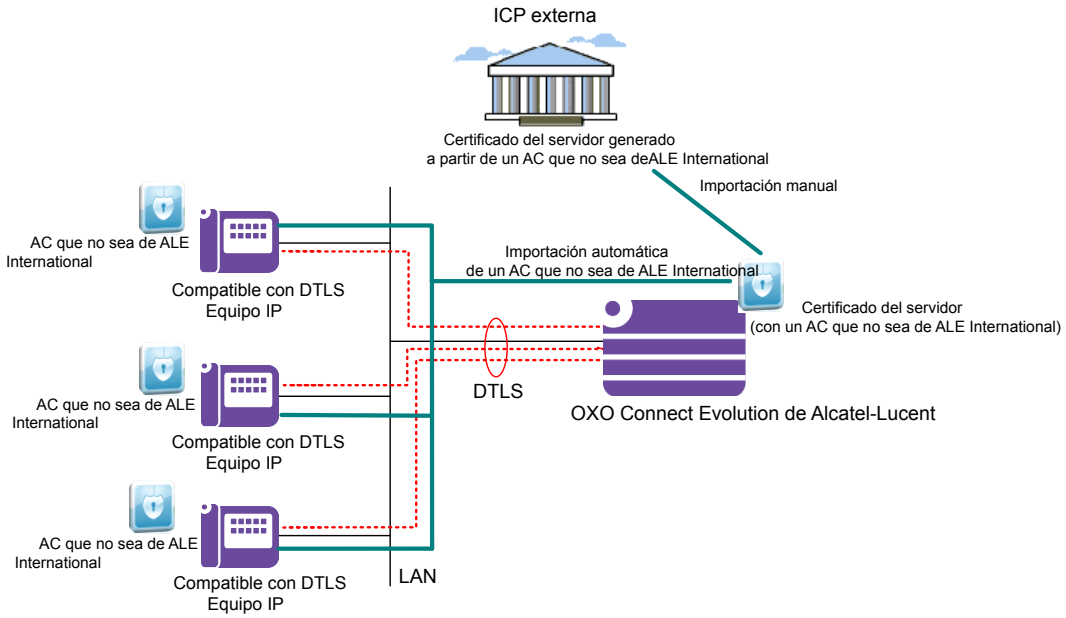
  > **Importante:**
  > Se recomienda hacer una copia de seguridad de la CA de Alcatel-Lucent Enterprise y los pares de claves correspondientes en una tarjeta SD extraíble. Al hacerla, esta copia se encriptará para proteger la clave privada.

- El parámetro **Aprovisionamiento automático de la TrustList de extremos** está habilitado en la PBX (opción predeterminada) (consulte Habilitar/deshabilitar la implementación automática de la CTL (Aprovisionamiento automático de la TrustList de extremos) *(en la página 21)*)
- El parámetro **Autenticación de extremos** debe deshabilitarse en la PBX mediante la aplicación **OMC** (consulte Activar/desactivar la autenticación de los extremos *(en la página 22)*)

En el modo DTLS forzada, los dispositivos IP sin capacidad DTLS no son compatibles con la PBX y se marcan como físicamente fuera de servicio.

Los dispositivos IP compatibles con DTLS recuperan automáticamente la CTL (incluida la CA externa) a través del archivo `lanpbx.cfg`, descargado desde la PBX. Por defecto, la primera adquisición de la CTL se lleva a cabo mediante el mecanismo **Aprovisionamiento automático de la TrustList de extremos**. La CTL recibida a través del archivo `lanpbx.cfg` se almacena en el almacenamiento de confianza del dispositivo IP compatible con DTLS.

En la negociación de la sesión DTLS, los dispositivos IP compatibles con DTLS autentican el certificado de servidor enviado por la PBX con la CTL almacenada en su almacenamiento de confianza. Tras la autenticación, los dispositivos IP compatibles con DTLS establecen una conexión DTLS segura con la PBX a través de la LAN.



Capítulo 3 Cifrado nativo

Los dispositivos IP compatibles con DTLS se pueden mover de esta PBX segura a otra PBX, siempre que cumplan con las reglas descritas: Mover dispositivos IP de una PBX a otra *(en la página 25)*.

3.3.4. Cifrado nativo con autenticación de extremos

En esta configuración, el cliente busca que la PBX autentique los dispositivos IP compatibles con DTLS durante la conexión DTLS (consulte Autenticación del servidor y el cliente para las conexiones DTLS *(en la página 11)*). Por defecto, la autenticación de extremos está habilitada en el modo **experto** (consulte Activar/desactivar la autenticación de los extremos *(en la página 22)*).

Cuando la autenticación de extremos se habilita en la PBX, la autenticación del dispositivo IP se basa en la autoridad de certificación del terminal Alcatel (establecido en el almacenamiento de confianza de la PBX: consulte Autoridad de certificación del terminal ALE *(en la página 65)* para obtener más información) o en un certificado específico generado por una PKI externa. En este caso, este certificado específico emitido desde una autoridad de certificación que no sea deAlcatel-Lucent Enterprise debe importarse manualmente al dispositivo IP compatible con DTLS a través de MMI local, mientras que la autoridad de certificación que no sea de Alcatel-Lucent Enterprise que emitió el certificado específico debe importarse a la PBX a través de la Web-Based Tool (véase: Configurar los certificados en la PBX *(en la página 24)*).

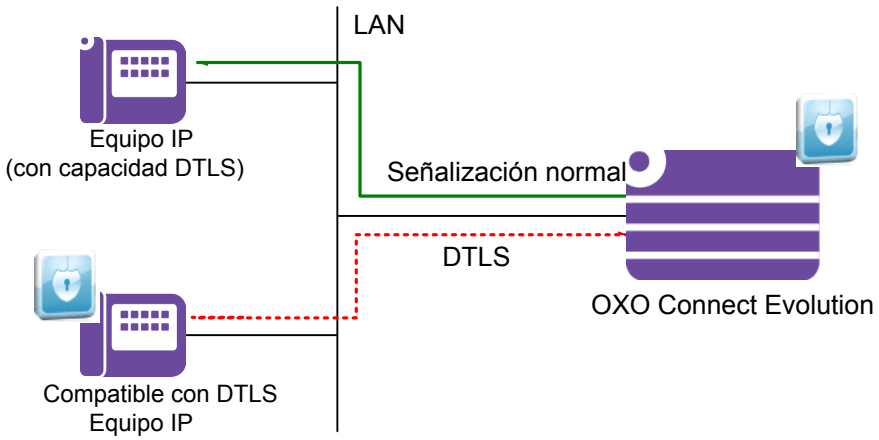
Atención:
El cliente de IP Desktop Softphone no añade ningún certificado predeterminado. Si se activa la autenticación de extremos en la PBX, los clientes de IP Desktop Softphone deben personalizarse primero con un certificado generado por una PKI externa.

Nota:
Para autenticar correctamente los dispositivos IP, los certificados de dispositivo IP deben generarse con la dirección MAC del dispositivo IP configurado en el campo «Nombre común».

3.3.5. Compatibilidad de dispositivos IP sin capacidad DTLS

La instalación del cliente puede contener dispositivos IP compatibles con DTLS y dispositivos IP sin capacidad DTLS.

Los dispositivos IP compatibles con DTLS establecen un enlace de señalización seguro (conexión DTLS) con la PBX a través de la LAN, mientras que los dispositivos IP sin capacidad DTLS establecen un enlace de señalización no seguro con la PBX (modo sin cifrado).



Capítulo 3 Cifrado nativo

Esta configuración no se recomienda para proporcionar un entorno seguro completo.

En el modo **experto**, es posible forzar la PBX para que solo acepte un enlace de señalización seguro a través de DTLS si se configura el parámetro **Modo DTLS forzado** en la configuración de la PBX (consulte Activar/desactivar el modo DTLS forzada *(en la página 23)*). En este caso, todos los dispositivos IP (sin capacidad DTLS) ya no pueden conectarse a la PBX.

En el modo **estándar**, todos los dispositivos IP pueden conectarse a la PBX, incluidos los dispositivos IP sin capacidad DTLS. El parámetro **Modo DTLS forzado** esta deshabilitado y no puede modificarse en la configuración de la PBX.

3.4. Configuración de cifrado nativo

Este capítulo describe la configuración del **cifrado nativo** en la PBX (OXO Connect Evolution).

En OMC, la pantalla **cifrado DTLS** se emplea para configurar el **cifrado nativo**. Esta pantalla se abre:

- En el **modo estándar**, cuando la PBX utiliza el certificado genérico para su autenticación en la conexión DTLS
- En el **modo experto**, cuando la PBX usa un certificado específico con una autoridad de certificación que no sea de Alcatel-Lucent Enterprise para la autenticación en la conexión DTLS

El valor predeterminado de los campos del **cifrado DTLS** varía según el modo utilizado:

Campo	Modo estándar	Modo Experto
Cifrado DTLS	Activado	Activado
Aprovisionamiento automático de la TrustList de extremos	Activado (*)	Activado
Autenticación de los extremos	Desactivado (*)	Activado
Modo DTLS activado	Desactivado (*)	Activado
Restablecer la TrustList de extremos	Deshabilitado	Deshabilitado

(*): en modo **estándar**, estos campos no se pueden modificar.

Capítulo 3 Cifrado nativo

3.4.1. Activar/desactivar cifrado nativo en modo estándar

Tras la instalación de la PBX, el **cifrado nativo** se habilita por defecto en el modo **estándar**. Para activar/desactivar el **cifrado nativo** en la PBX:

1. En OMC, seleccione **Seguridad** > **Cifrado DTLS**
2. Revise/modifique el siguiente campo:

Cifrado DTLS	• **Activado** (opción predeterminada): el **cifrado nativo** está activado en la PBX y todos los dispositivos IP compatibles con DTLS. • **Desactivado**: el **cifrado nativo** está desactivado en la PBX y todos los dispositivos IP compatibles con DTLS. Después de modificar este campo, se le solicitará reiniciar todos los dispositivos IP compatibles con DTLS. Haga clic en **Sí** para iniciar la operación.

3. Haga clic en **OK** para validar

Nota:
El resto de campos del **cifrado nativo** aparecen en color gris y no se pueden modificar. Para más información sobre el significado de los campos del **cifrado nativo**, consulte Configurar el cifrado nativo en modo experto *(en la página 20)*.

3.4.2. Configurar el cifrado nativo en modo experto

3.4.2.1. Activar/desactivar cifrado nativo en modo experto

Tras la instalación de la PBX, el **cifrado nativo** se habilita en el modo **experto** cuando se implementa un certificado específico en la PBX. Para activar/desactivar el **cifrado nativo** en la PBX:

1. En OMC, seleccione **Seguridad** > **Cifrado DTLS**
2. Revise/modifique el siguiente campo:

Cifrado DTLS	• **Activado** (opción predeterminada): el **cifrado nativo** está activado en la PBX y todos los dispositivos IP compatibles con DTLS. • **Desactivado**: el **cifrado nativo** está desactivado en la PBX y todos los dispositivos IP compatibles con DTLS. Después de modificar este campo, se le solicitará reiniciar todos los dispositivos IP compatibles con DTLS. Haga clic en **Sí** para iniciar la operación.

3. Haga clic en **OK** para validar

3.4.2.2. Activar/desactivar el cifrado nativo para determinados dispositivos IP compatibles con DTLS

Tras la instalación de la PBX, el **cifrado nativo** se activa por defecto para todos los dispositivos IP compatibles con DTLS. Es posible activar o desactivar el **cifrado nativo** para un dispositivo IP compatible con DTLS determinado:

1. En OMC, seleccione **Lista de usuarios/estaciones base**
2. Seleccione el dispositivo IP compatible con DTLS que desee y, a continuación, seleccione **Detalles** > **IP/SIP**
3. Revise/modifique el siguiente campo:

Cifrado DTLS	Este campo solo es aplicable si el **cifrado nativo** está activado en la PBX. Este campo aparece en gris y no se puede modificar para los dispositivos IP que no son compatibles con el cifrado DTLS o para los dispositivos IP conectados a una versión de OXO Connect Evolution anterior a R3.1. • **Activado** (opción predeterminada): el **cifrado nativo** está activado en lel dispositivo IP compatible con DTLS. La conexión entre el dispositivo IP y la PBX está cifrada (conexión DTLS). • **Desactivado**: el **cifrado nativo** está desactivado en el dispositivo IP compatible con DTLS. El dispositivo IP recibe un mensaje específico de la PBX a través del enlace de señalización aún cifrado. DTLS está desactivado y la conexión entre el dispositivo IP y la PBX ya no está cifrada (modo sin cifrado).

4. Haga clic en **OK** para validar

3.4.2.3. Habilitar/deshabilitar la implementación automática de la CTL (Aprovisionamiento automático de la TrustList de extremos)

Tras la instalación de la PBX, los dispositivos IP compatibles con DTLS recuperan automáticamente la CTL (incluida la CA genérica) a través del archivo `lanpbx.cfg`, descargado desde la PBX. Por defecto, la implementación automática de la CTL es´ta habilitada en la PBX: la adquisición de la CTL se lleva a cabo mediante el mecanismo **Aprovisionamiento automático de la TrustList de extremos**.

Para habilitar/deshabilitar la implementación automática de la CTL desde la PBX:

1. En OMC, seleccione **Seguridad** > **Cifrado DTLS**
2. Revise/modifique el siguiente campo:

Aprovisionamiento automático de la TrustList de extremos	• **Activado** (opción predeterminada): la CTL de la PBX se añadirá automáticamente al archivo `lanpbx.cfg` descargado por los dispositivos IP compatibles con DTLS. • **Desactivado**: la CTL de la PBX no se incluirá en el archivo `lanpbx.cfg` cargado por los dispositivos IP compatibles con DTLS. La CTL de la PBX debe cargarse manualmente en los dispositivos IP compatibles con DTLS. Después de modificar este campo, se le solicitará reiniciar los dispositivos IP compatibles con DTLS. Haga clic en **Sí** para iniciar la operación.

3. Haga clic en **OK** para validar

3.4.2.4. Activar/desactivar la autenticación de los extremos

1. En OMC, seleccione **Seguridad** > **Cifrado DTLS**
2. Revise/modifique el siguiente campo:

Autenticación de los extremos	• **Activado** (opción predeterminada): la autenticación de los extremos (servidor y cliente) se aplica a las conexiones DTLS. Los dispositivos IP compatibles con DTLS autentican la PBX y esta, a su vez, autentica los dispositivos IP compatibles con DTLS (consulte Autenticación del servidor y el cliente para las conexiones DTLS *(en la página 11)*). • **Desactivado**: la autenticación del servidor se aplica a las conexiones DTLS. Los dispositivos IP compatibles con DTLS solo autentican la PBX. Modificar este campo requiere un reinicio en caliente de la PBX

3. Haga clic en **OK** para validar

3.4.2.5. Activar/desactivar el modo DTLS forzada

1. En OMC, seleccione **Seguridad** > **Cifrado DTLS**
2. Revise/modifique el siguiente campo:

Modo DTLS activado	• **Activado** (opción predeterminada): solo los dispositivos IP compatibles con DTLS pueden conectarse a la PBX. • **Desactivado**: todos los dispositivos IP pueden conectarse a la PBX, incluidos aquellos que no son compatibles con DTLS: el enlace de señalización entre estos dispositivos IP y la PBX no está cifrado (modo sin cifrado).

3. Haga clic en **OK** para validar

3.4.3. Activar/desactivar el reinicio de la CTL de todos los dispositivos IP compatibles con DTLS

1. En OMC, seleccione **Seguridad** > **Cifrado DTLS**
2. Revise/modifique el siguiente campo:

Restablecer la TrustList de extremos	Este campo se puede modificar cuando el campo de **cifrado DTLS** está desactivado. • **Activado**: la CTL de cada dispositivo IP compatible con DTLS se restablece automáticamente (se borra la información de la CTL). • **Desactivado** (opción predeterminada): no se restablece automáticamente la CTL de cada dispositivo IP compatible con DTLS. Después de modificar este campo, se le solicitará reiniciar los dispositivos IP compatibles con DTLS. Haga clic en **Sí** para iniciar la operación.

3. Haga clic en **OK** para validar

3.4.4. Configurar los certificados en la PBX

La gestión de certificados para el **cifrado nativo** se lleva a cabo mediante la Web-Based Tool (ruta de acceso: **Certificados** > **Certificado DTLS**). Desde la Web-Based Tool, puede realizar las siguientes operaciones:

- Generar un certificado de servidor nuevo a partir de la autoridad de certificación genérica de Alcatel-Lucent Enterprise

  Si el certificado de servidor actual en la PBX es un certificado específico, esta operación permite reemplazar el certificado de servidor por un certificado de servidor nuevo, generado a partir de la autoridad de certificación de Alcatel-Lucent Enterprise.

- Importar a la PBX un certificado de servidor específico (y su autoridad de certificación que no sea de Alcatel-Lucent Enterprise) generado a partir de una PKI externa

  Una vez que el certificado de servidor específico esté firmado por una autoridad de certificación que no sea de Alcatel-Lucent Enterprise, debe importarse a la PBX con el certificado de la autoridad de certificación que no sea de Alcatel-Lucent Enterprise que emitió el certificado de servidor específico. Los formatos autorizados para archivos de certificado específicos emitidos desde una CA externa son PKCS#12/PKCS#7.

  Se requiere un reinicio en caliente de la PBX para reemplazar el certificado de servidor actual por el certificado de servidor nuevo. Tras el reinicio, la PBX estará en modo **experto** y usará este certificado de servidor nuevo para la autenticación en la conexión DTLS

  > **Nota:**
  > La autoridad de certificación que no sea de Alcatel-Lucent Enterprise también debe importarse en la CTL de los dispositivos IP compatibles con DTLS, ya sea a través de la MMI local o el mecanismo **Aprovisionamiento automático de la TrustList de extremos**.

- Importar a la PBX las autoridades de certificación que no sean de Alcatel-Lucent Enterprise que hayan emitido los certificados de dispositivos IP compatibles con DTLS

  Esta operación aborda las conexiones DTLS con autenticación de extremos (dispositivos IP compatibles con PBX y DTLS). Es necesaria cuando la casilla **Autenticación de extremos** se ha configurado en la configuración de la PBX (consulte Activar/desactivar la autenticación de los extremos *(en la página 22)*).

Para obtener más información sobre la gestión de certificados desde la Web-Based Tool, consulte el documento [9].

Capítulo 3 Cifrado nativo

3.5. Mantenimiento del cifrado nativo

3.5.1. Mover dispositivos IP de una PBX a otra

- Cuando los dispositivos IP compatibles con DTLS deben moverse de una PBX protegida a una PBX no protegida, antes debe realizar cualquiera de las siguientes operaciones:
  - Desactivar el **cifrado nativo** en la PBX (consulte Activar/desactivar cifrado nativo en modo experto *(en la página 20)*) y activar el reinicio automático de la CTL de todos los dispositivos IP (consulte Activar/desactivar el reinicio de la CTL de todos los dispositivos IP compatibles con DTLS *(en la página 23)*)

    Nota:
    Si el **cifrado nativo** se ha desactivado en los dispositivos IP (consulte Activar/desactivar el cifrado nativo para determinados dispositivos IP compatibles con DTLS *(en la página 21)*): es necesario reiniciar manualmente la CTL de todos los dispositivos IP (consulte el procedimiento más abajo)

  - Reinicie manualmente la CTL de los dispositivos IP (consulte el procedimiento más abajo)
- Cuando los dispositivos IP compatibles con DTLS deben moverse de una PBX segura a otra PBX segura:
  - Si las PBX incluyen certificados emitidos por la misma CA: los dispositivos IP pueden moverse sin ninguna configuración previa
  - Si las PBX incluyen certificados emitidos por diferentes CA: reinicie manualmente la CTL de los dispositivos IP (consulte el procedimiento más abajo)

Para reiniciar la CTL del dispositivo IP:

1. Conéctese al dispositivo IP compatible con DTLS a través de la MMI local (se requiere la contraseña de administrador de dispositivos: para más información sobre esta contraseña, véase Contraseña del administrador NOE IP *(en la página 82)*)
2. Reinicie al nivel predeterminado el dispositivo IP compatible con DTLS
3. Desconecte el dispositivo IP compatible con DTLS de la LAN. Si no lo hace, el dispositivo IP compatible con DTLS recupera la CTL de la PBX (a través del mecanismo **Aprovisionamiento automático de la TrustList de extremos**) y se bloquea en la PBX inicial
4. Reinicie con la nueva configuración el dispositivo IP compatible con DTLS

3.5.2. Desbloqueo de dispositivos IP mediante un token de recuperación

Es una procedimiento excepcional que debe llevar a cabo el equipo de asistencia de Alcatel-Lucent Enterprise.

Si el cliente utiliza un certificado personalizado y no puede guardar la clave privada ni la contraseña del administrador del teléfono correspondientes, si el sistema falla y no hay otra copia de seguridad disponible, los dispositivos IP compatibles con DTLS se bloquearán con el certificado actual del sistema. En este caso, el cliente debe ponerse en contacto con el fabricante del sistema para obtener ayuda.

Capítulo 3 *Cifrado nativo*

Bajo el control del equipo de asistencia de Alcatel-Lucent Enterprise, se recobra el token de recuperación, que debe importarse a la PBX mediante la Web-Based Tool (ruta de acceso: **Certificados** > **Token de recuperación DTLS**). Para obtener más información, consulte el documento [9].

Capítulo 4

Cifrado SIP-TLS/SRTP para enlaces SIP

4.1. Descripción general de SIP-TLS/SRTP para enlaces SIP

A partir de R3.2, los protocolos SIP-TLS y SRTP son compatibles para cifrar las comunicaciones en enlaces SIP públicos y privados:

- Los flujos de señalización entre la PBX (OXO Connect Evolution) y los componentes SIP remotos (públicos o privados) se cifran mediante SIP-TLS. SIP-TLS permite la autenticación de la PBX y los componentes remotos SIP a través del intercambio de certificados.
- Los flujos de medios entre la PBX y los componentes SIP remotos se cifran mediante SRTP. Esto se aplica a flujos de medios como: voz, DTMF y fax a través de G.711.

En los enlaces SIP públicos, las comunicaciones entre la PBX y la pasarela del operador SIP se cifran mediante la red WAN.

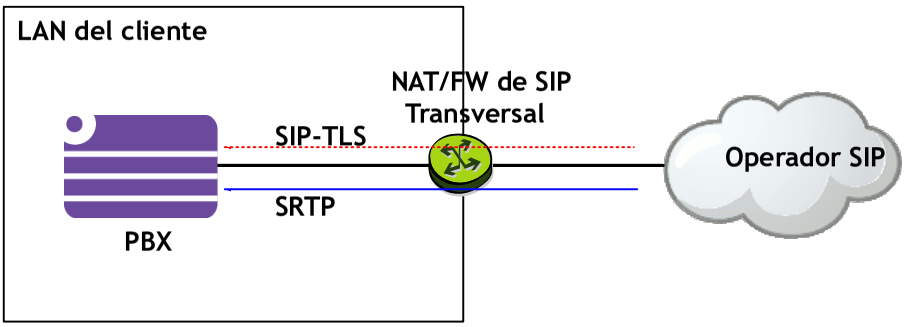


Figura 4-1 Cifrado de comunicaciones en enlaces SIP públicos

Capítulo 4 Cifrado SIP-TLS/SRTP para enlaces SIP

En los enlaces SIP privados, las comunicaciones entre la PBX y los componentes SIP remotos (como la pasarela de medios, el servidor de fax u otra PBX) se cifran mediante una red WAN o LAN.

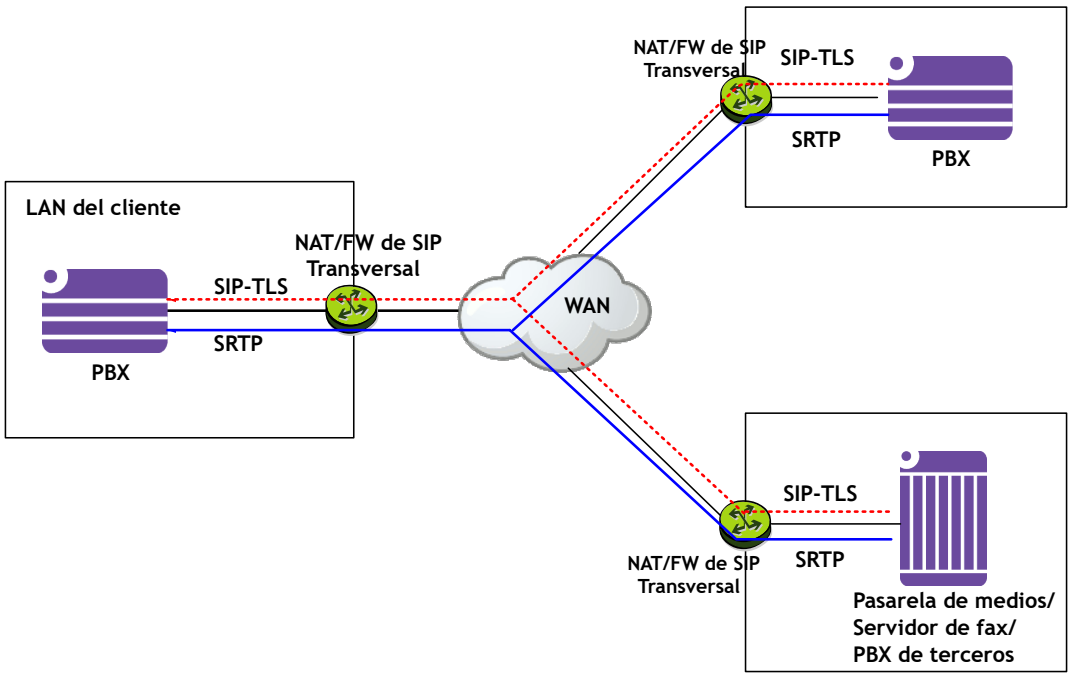


Figura 4-2 Cifrado de comunicaciones en enlaces SIP privados (mediante red WAN)

Si la PBX se conecta a los clientes de Rainbow mediante una pasarela WebRTC, no existirá cifrado SIP-TLS / SRTP en el enlace SIP establecido entre la PBX y la pasarela WebRTC.

El cifrado SIP-TLS/SRTP se activa y configura en la pasarela SIP de la PBX.

4.2. Descripción del cifrado SIP-TLS/SRTP

4.2.1. Cifrado SIP-TLS

SIP-TLS se utiliza para proteger los mensajes de señalización SIP: ofrece privacidad e integridad de datos de los mensajes de señalización SIP. TLS se superpone a un protocolo de transporte fiable TCP.

El cifrado SIP-TLS se activa y configura en los ajustes de la pasarela SIP de la PBX (véase: Activación y configuración de SIP-TLS en la pasarela SIP de la PBX *(en la página 37)*).

4.2.1.1. Autenticación SIP-TLS

La PBX es compatible con dos métodos de autenticación SIP-TLS:

- Autenticación de servidor con certificados *(en la página 29)*
- Autenticación mutua *(en la página 29)*

4.2.1.1.1. Autenticación de servidor con certificados

En la autenticación del servidor, el servidor TLS es el único que proporciona un certificado en la conexión a la sesión SIP-TLS:

- Cuando actúa como cliente TLS, la PBX inicia la conexión con TLS: el servidor TLS proporciona a la PBX el certificado de autenticación. La CA del servidor debe figurar en el repositorio de certificados de confianza de la PBX para poder autenticar el certificado del servidor.
- Cuando actúa como servidor TLS, la PBX proporciona a la PBX el certificado de autenticación al cliente TLS. La CA de la PBX debe figurar en el repositorio de certificados de confianza del cliente para poder autenticar el certificado de la PBX.

4.2.1.1.2. Autenticación mutua

En la autenticación mutua, el servidor TLS y el cliente proporcionan un certificado en la conexión a la sesión SIP-TLS:

- Cuando actúa como cliente TLS, la PBX siempre recibe certificado del servidor para la autenticación. En lo que respecta al servidor, si la autenticación mutua está habilitada, solicita el certificado del cliente para la autenticación: la PBX proporciona el certificado al servidor. La autoridad de certificación (CA) de la PBX debe figurar en el repositorio de certificados de confianza del servidor para poder autenticar el certificado de la PBX.
- Cuando actúa como servidor TLS, la PBX recibe el certificado del cliente para la autenticación, siempre que el parámetro de **autenticación mutua** se haya activado en la configuración de la PBX (véase: Activación y configuración de SIP-TLS en la pasarela SIP de la PBX *(en la página 37)*). Si está habilitado, solicita el certificado del cliente para la autenticación. La CA del cliente debe figurar en el repositorio de certificados de confianza de la PBX para poder autenticar el certificado del cliente.

Para llevar a cabo la migración desde OXO Connect Evolution R3.1 o inferior hasta R3.2 o superior, el certificado TLS se debe generar en la PBX que actúa como cliente TLS para que la autenticación mutua sea correcta. El certificado TLS se debe generar manualmente con la Web-Based Tool. Consulte el documento [3] para obtener información sobre cómo generar el certificado TLS.

Cuando la autenticación mutua está habilitada pero no se ha generado un certificado TLS, el protocolo de enlace TLS falla y la conexión se interrumpe debido a un error de certificado incorrecto.

4.2.1.2. Certificados utilizados para la autenticación de SIP-TLS

La autenticación SIP-TLS se basa en certificados que utilizan algoritmos criptográficos solidos. Los certificados implementados en la PBX pueden ser:

- Certificados dinámicos firmados por la autoridad de certificación local (CA)

  Por defecto, cada PBX incluye una única autoridad de certificación local (CA). Durante la instalación, la PBX genera automáticamente su propio certificado dinámico a partir de esta autoridad de certificación local. El certificado dinámico se vuelve a generar cuando se produce una de las siguientes condiciones:

  - La dirección IP de la PBX/nombre de host cambia
  - La dirección IP del enrutador de acceso cambia
  - Se realiza una solicitud manual a través de la Web-Based Tool

Para más información sobre los certificados dinámicos, véase: Certificado dinámico *(en la página 49)*

- Certificados personalizados firmados por una CA que no es de Alcatel-Lucent Enterprise

  Este certificado personalizado se gestiona independientemente de la PBX. Se debe importar en la PBX junto con el certificado de la CA que no sea de Alcatel-Lucent Enterprise que emitió el certificado personalizado.

  Para más información sobre los certificados personalizados, véase: Certificados personalizados *(en la página 51)*

La gestión de todos los certificados se lleva a cabo mediante la Web-Based Tool (sesión del instalador o el fabricante). Para obtener más detalles, consulte Configuración de certificados de la PBX *(en la página 40)*.

4.2.1.3. Lista de certificados de confianza (CTL) de la PBX

Se configura una lista de certificados de confianza (CTL) en la PBX. Contiene las CA que emitieron los certificados de dispositivos SIP remotos.

Para permitir que los dispositivos SIP remotos autentiquen la PBX durante las conexiones SIP-TLS, esta CTL debe implementarse en el repositorio de certificados de confianza de los dispositivos SIP remotos, y viceversa.

La gestión del almacén de confianza de la PBX se lleva a cabo mediante la Web-Based Tool (sesión del instalador o el fabricante). Para obtener más detalles, consulte Configuración del repositorio de certificados de confianza de la PBX *(en la página 40)*.

4.2.2. Cifrado SRTP

SRTP es una extensión del perfil RTP, especificado por RFC3711: ofrece características de seguridad, como la autenticación de paquetes, confidencialidad y la protección de reproducción para flujos de medios. Se utiliza para proteger los paquetes RTP y los paquetes RTCP.

SRTP define un conjunto de transformaciones criptográficas predeterminadas. Cuando se usa junto con un sistema de gestión de claves adecuado, ofrece una seguridad sólida. La PBX implementa RFC4568 para configurar esta gestión de claves.

El cifrado SRTP se activa y configura en los ajustes de la pasarela SIP de la PBX (véase: Activación y configuración de SRTP en la pasarela SIP de la PBX *(en la página 41)*).

SRTP solo se puede configurar si SIP-TLS está habilitado en la pasarela SIP de la PBX.

4.3. Topologías del cifrado SIP-TLS/SRTP para enlaces SIP

4.3.1. Cifrado SIP-TLS/SRTP entre la PBX y el operador SIP

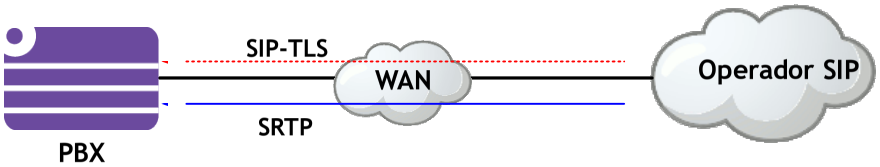


Figura 4-3 Cifrado SIP-TLS/SRTP entre la PBX y el operador SIP

Capítulo 4 Cifrado SIP-TLS/SRTP para enlaces SIP

Se genera un enlace SIP entre la PBX y un operador SIP a través de la red IP pública. El operador SIP espera el registro de SIP: la PBX está configurada para enviar una solicitud de `REGISTRO` con las credenciales proporcionadas por el operador de SIP. Puesto que la PBX siempre envía la solicitud de `REGISTRO` al operador SIP, siempre actúa como cliente TLS. Cuando se envía la solicitud de `REGISTRO` para establecer una conexión SIP-TLS, la PBX inicia la negociación de la sesión TLS. Cuando actúa como servidor TLS, el operador SIP proporciona el certificado a la PBX para su autenticación. Una vez la autenticación ha finalizado, se establece una conexión TLS segura. Esta conexión TLS se usa para llamadas entrantes y salientes. La conexión TLS se mantiene utilizando el mecanismo «mantener activo» de la SIP.

Los flujos de medios entre la PBX y el operador SIP están cifrados mediante SRTP.

El siguiente procedimiento de configuración debe realizarse en la PBX y NAT/Firewall para el cifrado SIP-TLS/SRTP:

- El SIP-TLS se debe activar y configurar en los ajustes de la pasarela SIP de la PBX (véase: Activación y configuración de SIP-TLS en la pasarela SIP de la PBX *(en la página 37)*).
- El puerto utilizado para la conexión a SIP-TLS se debe configurar en la PBX (véase: Configuración del puerto para SIP-TLS *(en la página 38)*). La NAT/firewall transversal correspondiente para el puerto SIP-TLS se debe procesar en el enrutador de la CPE.
- Para mantener la conexión SIP-TLS, el parámetro **mantener activo** se debe establecer en la **opción SIP** en los ajustes de la pasarela SIP de la PBX (véase: Configuración de la opción «mantener activo» de SIP-TLS (opcional) *(en la página 39)*). El valor de tiempo de espera del parámetro «mantener activo» no debe superar los 300 segundos, que es el valor predeterminado.
- La CA del operador SIP se debe importar en el repositorio de certificados de confianza de la PBX (véase: Configuración del repositorio de certificados de confianza de la PBX *(en la página 40)*).
- El SRTP se debe activar y configurar en los ajustes de la pasarela SIP de la PBX (véase: Activación y configuración de SRTP en la pasarela SIP de la PBX *(en la página 41)*).

Nota:
La autenticación mutua no se aplica a esta configuración porque la PBX siempre actúa como cliente TLS.

4.3.2. Cifrado SIP-TLS/SRTP entre dos PBX en WAN

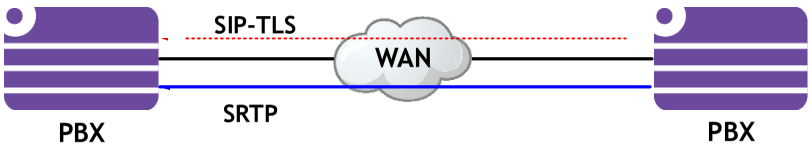


Figura 4-4 Cifrado SIP-TLS/SRTP entre dos PBX en WAN

Se genera un enlace SIP entre las dos PBX a través de la red WAN. La PBX no actúa como registrador, y ninguna de las dos PBX ha enviado mensajes de `REGISTRO`. El establecimiento de la conexión TLS se basa en la solicitud inicial `INVITAR/OPCIONES`, que se puede enviar desde cualquier dirección. La central que inicia la solicitud se convierte en el cliente TLS, mientras que la otra central se convierte en el servidor TLS.

Cuando actúa como servidor TLS, la PBX proporciona el certificado al cliente para su autenticación. Si la autenticación mutua está habilitada, la PBX solicita el certificado del cliente para su autenticación.

Capítulo 4 Cifrado SIP-TLS/SRTP para enlaces SIP

Los flujos de medios entre ambas PBX están cifrados mediante SRTP. Esta topología no requiere el establecimiento de un enlace VPN para asegurar los intercambios entre las PBX.

El siguiente procedimiento de configuración debe realizarse en ambas PBX y NAT/Firewall para el cifrado SIP-TLS/SRTP:

- El SIP-TLS se debe activar y configurar en los ajustes de la pasarela SIP de las PBX (véase: Activación y configuración de SIP-TLS en la pasarela SIP de la PBX *(en la página 37)*).
- El puerto utilizado para la conexión a SIP-TLS se debe configurar en las PBX (véase: Configuración del puerto para SIP-TLS *(en la página 38)*). La NAT/firewall transversal correspondiente para el puerto SIP-TLS se debe procesar en el enrutador de la CPE.
- La NAT estática debe activarse y configurarse en Configuración de la NAT estática *(en la página 39)*. La dirección IP pública y el puerto que se utiliza para SIP-TLS en el enrutador CPE deben configurarse en el NAT estático de las PBX.
- Se recomienda habilitar la autenticación mutua en las dos PBX (véase Activación y configuración de SIP-TLS en la pasarela SIP de la PBX *(en la página 37)*)
- Para mantener la conexión SIP-TLS, el parámetro **mantener activo** se debe establecer en la **opción SIP** en los ajustes de la pasarela SIP de las PBX (véase: Configuración de la opción «mantener activo» de SIP-TLS (opcional) *(en la página 39)*). El valor de tiempo de espera del parámetro «mantener activo» no debe superar los 300 segundos, que es el valor predeterminado.
- La CA de la primera PBX se debe importar en el repositorio de certificados de confianza de la PBX y viceversa (véase: Configuración del repositorio de certificados de confianza de la PBX *(en la página 40)*).
- El SRTP se debe activar y configurar en los ajustes de la pasarela SIP de la PBX (véase: Activación y configuración de SRTP en la pasarela SIP de la PBX *(en la página 41)*).

4.3.3. Cifrado SIP-TLS/SRTP entre la PBX y la pasarela de medios/PBX de terceros en WAN

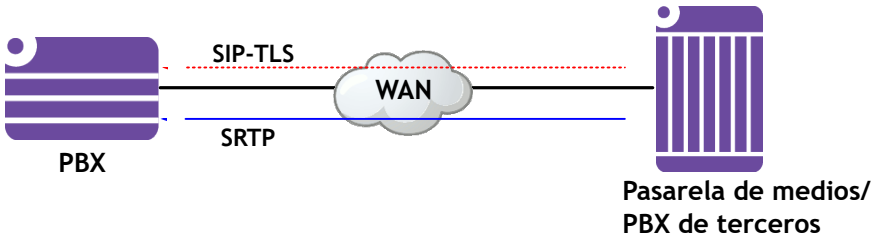


Figura 4-5 Cifrado SIP-TLS/SRTP entre la PBX y la pasarela de medios/PBX de terceros

Se genera un enlace SIP entre la PBX y la pasarela de medios/PBX de terceros a través de la red WAN. La PBX no actúa como registrador, y no se envía ningún mensaje de `REGISTRO` desde la pasarela de medios (u otra PBX de terceros) a la PBX. El establecimiento de la conexión TLS se basa en la solicitud inicial `INVITAR/OPCIONES`, que se puede enviar desde cualquier dirección.

Cuando actúa como servidor TLS, la PBX proporciona el certificado al cliente para su autenticación. Si la autenticación mutua está habilitada, la PBX solicita el certificado del cliente para su autenticación.

Nota:
La pasarela de medios/PBX de terceros pueden actuar como cliente TLS o servidor TLS.

Capítulo 4 *Cifrado SIP-TLS/SRTP para enlaces SIP*

Los flujos de medios entre la PBX y la pasarela de medios/PBX de terceros están cifrados mediante SRTP.

El siguiente procedimiento de configuración debe realizarse en la PBX y NAT/Firewall para el cifrado SIP-TLS/SRTP:

- El SIP-TLS se debe activar y configurar en los ajustes de la pasarela SIP de la PBX (véase: Activación y configuración de SIP-TLS en la pasarela SIP de la PBX *(en la página 37)*).
- El puerto utilizado para la conexión a SIP-TLS se debe configurar en la PBX (véase: Configuración del puerto para SIP-TLS *(en la página 38)*). La NAT/firewall transversal correspondiente para el puerto SIP-TLS se debe procesar en el enrutador de la CPE.
- La NAT estática debe activarse y configurarse en la PBX (véase: Configuración de la NAT estática *(en la página 39)*). La dirección IP pública y el puerto que se utiliza para SIP-TLS en el enrutador CPE deben configurarse en el NAT estático de la PBX.
- Se recomienda habilitar la autenticación mutua en la PBX (véase Activación y configuración de SIP-TLS en la pasarela SIP de la PBX *(en la página 37)*)
- Para mantener la conexión SIP-TLS, el parámetro **mantener activo** se debe establecer en la **opción SIP** en los ajustes de la pasarela SIP de la PBX (véase: Configuración de la opción «mantener activo» de SIP-TLS (opcional) *(en la página 39)*). El valor de tiempo de espera del parámetro «mantener activo» no debe superar los 300 segundos, que es el valor predeterminado.
- La CA de la pasarela de medios/PBX de terceros se debe importar en el repositorio de certificados de confianza de la PBX y viceversa (véase: Configuración del repositorio de certificados de confianza de la PBX *(en la página 40)*).
- El SRTP se debe activar y configurar en los ajustes de la pasarela SIP de la PBX (véase: Activación y configuración de SRTP en la pasarela SIP de la PBX *(en la página 41)*).

Restricción:

La pasarela de medios/PBX de terceros que solo tengan capacidad de cliente TLS no son compatibles, ya que existe la posibilidad de que la solicitud se inicie desde la PBX. En este caso, no será posible establecer la conexión TLS. Para corregir esta restricción, se requiere el siguiente procedimiento de configuración:

- La solicitud de **opción SIP** no se debe haber configurado en la pasarela de medios/PBX de terceros.

  La solicitud de **opción SIP** se activa desde la pasarela de medios (u otra PBX de terceros) hasta la PBX. La solicitud de **opción SIP** no se debe haber configurado en la pasarela SIP de la PBX.
- La autenticación mutua debe estar deshabilitada en la PBX.

  Esto garantiza que la pasarela de medios/PBX de terceros con capacidad de cliente TLS siempre actúe como cliente TLS: la solicitud de **opción SIP** se activa desde la pasarela de medios (u otra PBX de terceros) hasta la PBX que actúa como servidor TLS.

4.3.4. Cifrado SIP-TLS/SRTP entre la PBX y la pasarela de medios/servidor de fax en LAN

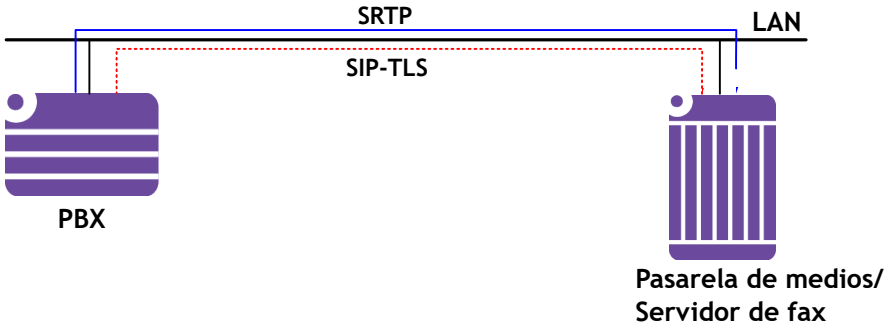


Figura 4-6 Cifrado SIP-TLS/SRTP entre la PBX y la pasarela de medios/servidor de fax

Se genera un enlace SIP entre la PBX y la pasarela de medios/servidor de fax a través de la red LAN. La PBX no actúa como registrador, y no se envía ningún mensaje de `REGISTRO` desde la pasarela de medios (o un servidor de fax) a la PBX. El establecimiento de la conexión TLS se basa en la solicitud inicial `INVITAR/OPCIONES`, que se puede enviar desde cualquier dirección.

Cuando actúa como servidor TLS, la PBX proporciona el certificado al cliente para su autenticación. Si la autenticación mutua está habilitada, la PBX solicita el certificado del cliente para su autenticación.

Nota:
La pasarela de medios/servidor de fax pueden actuar como cliente TLS o servidor TLS.

Los flujos de medios entre la PBX y la pasarela de medios/servidor de fax están cifrados mediante SRTP.

El siguiente procedimiento de configuración debe realizarse en la PBX para el cifrado SIP-TLS/SRTP:

- Se recomienda habilitar la autenticación mutua en la PBX (véase Activación y configuración de SIP-TLS en la pasarela SIP de la PBX *(en la página 37)*)
- Para mantener la conexión SIP-TLS, el parámetro **mantener activo** se debe establecer en la **opción SIP** en los ajustes de la pasarela SIP de la PBX (véase: Configuración de la opción «mantener activo» de SIP-TLS (opcional) *(en la página 39)*). El valor de tiempo de espera del parámetro «mantener activo» no debe superar los 300 segundos, que es el valor predeterminado.
- La CA de la pasarela de medios/PBX de terceros se debe importar en el repositorio de certificados de confianza de la PBX y viceversa (véase: Configuración del repositorio de certificados de confianza de la PBX *(en la página 40)*).
- El SRTP se debe activar y configurar en los ajustes de la pasarela SIP de la PBX (véase: Activación y configuración de SRTP en la pasarela SIP de la PBX *(en la página 41)*).

Restricción:

La pasarela de medios/servidor de fax que solo tengan capacidad de cliente TLS no son compatibles, ya que existe la posibilidad de que la solicitud se inicie desde la PBX. En este caso, no será posible establecer la conexión TLS. Para corregir esta restricción, se requiere el siguiente procedimiento de configuración:

- La solicitud de **opción SIP** no se debe haber configurado en la pasarela de medios/servidor de fax.

  La solicitud de **opción SIP** se activa desde la pasarela de medios (o un servidor de fax) hasta la PBX. La solicitud de **opción SIP** no se debe haber configurado en la pasarela SIP de la PBX.

- La autenticación mutua debe estar deshabilitada en la PBX.

  Esto garantiza que la pasarela de medios/PBX de terceros con capacidad de cliente TLS siempre actúe como cliente TLS: la solicitud de **opción SIP** se activa desde la pasarela de medios (o un servidor de fax) hasta la PBX que actúa como servidor TLS.

4.3.5. Cifrado SIP-TLS entre dos PBX en LAN

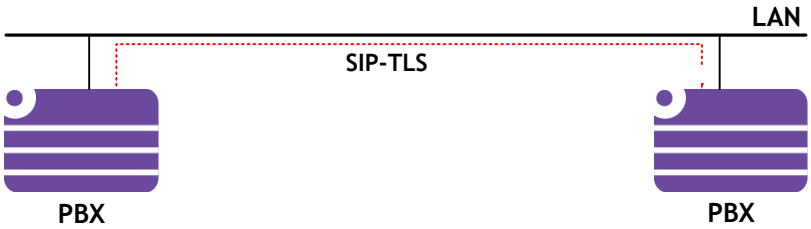


Figura 4-7 Cifrado SIP-TLS entre dos PBX en LAN

Se genera un enlace SIP entre las dos PBX a través de la red LAN. La PBX no actúa como registrador, y ninguna de las dos PBX ha enviado mensajes de `REGISTRO`. El establecimiento de la conexión TLS se basa en la solicitud inicial `INVITAR/OPCIONES`, que se puede enviar desde cualquier dirección. La central que inicia la solicitud se convierte en el cliente TLS, mientras que la otra central se convierte en el servidor TLS.

Cuando actúa como servidor TLS, la PBX proporciona el certificado al cliente para su autenticación. Si la autenticación mutua está habilitada, la PBX solicita el certificado del cliente para su autenticación.

El siguiente procedimiento de configuración debe realizarse en ambas PBX para establecer la consexión SIP-TLS:

- Se recomienda habilitar la autenticación mutua en las dos PBX (véase Activación y configuración de SIP-TLS en la pasarela SIP de la PBX *(en la página 37)*)
- Para mantener la conexión SIP-TLS, el parámetro **mantener activo** se debe establecer en la **opción SIP** en los ajustes de la pasarela SIP de las PBX (véase: Configuración de la opción «mantener activo» de SIP-TLS (opcional) *(en la página 39)*). El valor de tiempo de espera del parámetro «mantener activo» no debe superar los 300 segundos, que es el valor predeterminado.
- La CA de la primera PBX se debe importar en el repositorio de certificados de confianza de la PBX y viceversa (véase: Configuración del repositorio de certificados de confianza de la PBX *(en la página 40)*).

4.4. Configuración SIP-TLS/SRTP para enlaces SIP

En este capítulo, se describe la configuración SIP-TLS/SRTP para los enlaces SIP de la PBX (OXO Connect Evolution).

Capítulo 4 *Cifrado SIP-TLS/SRTP para enlaces SIP*

La siguiente configuración se aplica a enlaces SIP públicos y privados.

4.4.1. Requisitos previos

Los enlaces SIP deben configurarse en la PBX. Véase el documento [6] para obtener más información.

4.4.2. Configuración del cifrado SIP-TLS en la PBX

4.4.2.1. Activación y configuración de SIP-TLS en la pasarela SIP de la PBX

Para activar y configurar SIP-TLS en la pasarela SIP de la PBX:

1. En OMC, seleccione la pestaña **Líneas externas** > **SIP** > **Pasarelas SIP** > **Detalles de parámetros de pasarelas** >**Seguridad**
2. Revise/modifique los siguientes campos:

SIP TLS	Seleccione **Habilitado**: el cifrado SIP-TLS se activará en la pasarela SIP de la PBX. Valor predeterminado: **Deshabilitado** (el cifrado SIP-TLS estará desactivado en la pasarela SIP de la PBX).
Autenticación mutua	• **Habilitado**: la autenticación mutua (servidor y cliente) se aplica a las conexiones SIP-TLS. Los dispositivos SIP remotos autentican la PBX y, a su vez, la PBX autentica los dispositivos SIP remotos. • **Deshabilitado** (opción predeterminada): la autenticación del servidor se aplica a las conexiones DTLS. Los dispositivos SIP remotos solo autentican la PBX. Este campo solo se puede configurar cuando **SIP TLS** está habilitado. Si **SIP TLS** no está habilitado, esta casilla aparece deshabilitada y atenuada.
Admitir caracteres comodines en la extensión del certificado	• **Habilitado**: los certificados con caracteres comodín (por ejemplo: *.abc.com) se habilitan en la negociación de sesión SIP-TLS. • **Deshabilitado**: los certificados con caracteres comodín (por ejemplo: *.abc.com) no están permitidos en la negociación de sesión SIP-TLS. Este campo solo se puede configurar cuando **SIP TLS** está habilitado. Si **SIP TLS** no está habilitado, esta casilla aparece deshabilitada y atenuada.
SIPS URI	• **Habilitado** (valor predeterminado): OXO Connect Evolution envía el mensaje SIP con la URI de SIPS en todos los campos de título y espera de la URI de SIPS. De lo contrario, la llamada se rechazará. • **Deshabilitado**: OXO Connect Evolution envía el mensaje SIP con la URI de SIP en todos los campos de título y acepta tanto la URI de SIP como de SIPS en las solicitudes entrantes. Este campo solo se puede configurar cuando **SIP TLS** está habilitado. Si **SIP TLS** no está habilitado, esta casilla aparece deshabilitada y atenuada.

3. Haga clic en **OK** para validar

Nota:
Si **SIP TLS** está habilitado, el **Modo de transporte por defecto**, definido en la pestaña **Protocolo** de los **Detalles de parámetros de pasarelas**, cambia automáticamente a **SIP TLS** y no se puede configurar. Para cambiar el **Modo de transporte por defecto**, **SIP TLS** ha de estar inhabilitado.

4.4.2.2. Configuración del puerto para SIP-TLS

Debe configurarse el siguiente puerto para las conexiones SIP-TLS:

1. En OM, seleccione la pestaña **Voz sobre IP** > **VoIP: Parámetros** > **Enlace SIP**
2. Revise/modifique el siguiente campo:

Puerto de señal de enlaces SIP TLS	Introduzca el número del puerto en el que se establecen las conexiones SIP-TLS. Cualquier modificación de este valor obligará a reiniciar la PBX. Valor predeterminado: 5061 **Nota:** • En caso de restaurar la base de datos de R3.1 o de una versión inferior a R3.2 o superior, este campo recupera el valor predeterminado. • Este valor debe ser distinto de 0, del valor **Puerto de la señal del teléfono SIP** (ruta de acceso: **Voz sobre IP** >**Parámetros VoIP** > **Teléfono SIP**), y del **Puerto de señal de los enlaces SIP** configurados en esta pantalla. Se muestra una ventana emergente de advertencia si se produce algún problema durante la configuración del puerto.

3. Haga clic en **OK** para validar

4.4.2.3. Configuración de la NAT estática

Cuando la NAT estática se habilita para una pasarela SIP de la PBX con SIP-TLS, la dirección IP pública y el puerto que se usa para SIP-TLS en el enrutador CPE deben configurarse en la pasarela SIP de la PBX correspondiente.

1. En OMC, seleccione la pestaña **Líneas externas** > **SIP** > **Pasarelas SIP** > **Detalles de parámetros de pasarelas** >**Topología**
2. Revise/modifique el siguiente campo:

Puerto TLS SIP/SIP (UDP/TCP)	Introduzca el número de puerto UDP/TCP para el enrutador CPE de interfaz pública. Valor predeterminado: 5060

3. Haga clic en **OK** para validar

En caso de que el enlace SIP configurado sea dinámico, el valor `OPCIÓN` debe configurarse en la puerta de enlace SIP PBX (ruta de acceso en OMC: pestaña **Voz sobre IP** > **VoIP: Parámetros** > **Enlace SIP** > parámetro **sipgw_nat_ka**). Para obtener más información, consulte el documento [6].

Cuando se establece un enlace SIP entre una PBX y una pasarela de medios/servidor de fax con solo capacidad de cliente TLS, la solicitud de `OPCIÓN` solo debe configurarse en la pasarela de medios/ servidor de fax.

4.4.2.4. Configuración de la opción «mantener activo» de SIP-TLS (opcional)

Cuando SIP TLS está habilitado para una pasarela SIP de la PBX, se recomienda seleccionar la **opción SIP** en la configuración de la opción «mantener activo»:

1. En OMC, seleccione la pestaña **Líneas externas** > **SIP** > **Pasarelas SIP** > **Detalles de parámetros de pasarelas** >**Protocolo**
2. Revise/modifique los siguientes campos:

Alive Protocol	Seleccione **Opción SIP**.
Alive Timeout/s	Seleccione el tiempo de espera para comprobar la presencia del dispositivo SIP remoto. Valores posibles: 0 a 3600 segundos (valor predeterminado). 0: el mecanismo de "keep-alive" está desactivado.
Estado activo	Este campo de solo lectura muestra el estado del dispositivo SIP remoto (**Activo** o **Inactivo**)

3. Haga clic en **OK** para validar

4.4.2.5. Configuración de certificados de la PBX

La gestión de certificados para el cifrado SIP-TLS se lleva a cabo mediante la Web-Based Tool(ruta de acceso: **Certificados** > **Certificado de servidor**). Desde la Web-Based Tool, puede realizar las siguientes operaciones:

- Generar un certificado dinámico nuevo a partir de la autoridad de certificación local
- Importe a la PBX un certificado personalizado (y la CA que no sea de Alcatel-Lucent Enterprise). Una vez importado, el certificado personalizado podrá reemplazar al certificado dinámico actual.

El cambio de certificado requiere un reinicio en caliente de la PBX.

Para obtener más información sobre la gestión de certificados desde la Web-Based Tool, consulte el documento [9].

4.4.2.6. Configuración del repositorio de certificados de confianza de la PBX

La gestión del almacenamiento de confianza de la PBX para el cifrado SIP-TLS se lleva a cabo mediante la Web-Based Tool (ruta de acceso: **Certificados** > **Almacenamiento de confianza**). Desde la Web-Based Tool, puede importar a la PBX las CA que no sean de Alcatel-Lucent Enterprise que emitieron los certificados de dispositivos SIP remotos.

El repositorio de certificados de confianza de la PBX debe completarse en los siguientes casos de uso:

- Si la conexión SIP-TLS se establece entre una PBX y un operador SIP, el repositorio de certificados de confianza de la PBX debe completarse con la CA del operador SIP.
- Si la conexión SIP-TLS se establece entre una PBX1 y un dispositivo SIP remoto (PBX2, pasarela de medios o servidor de fax) a través de un enlace privado, el repositorio de certificados de confianza de la PBX1 debe completarse con la CA del dispositivo SIP remoto, mientras que el repositorio de certificados de confianza del dispositivo SIP remoto debe completarse con la CA de la PBX1.

Para obtener más información sobre la gestión de almacenamiento de confianza desde la Web-Based Tool, consulte el documento [9].

4.4.3. Activación y configuración de SRTP en la pasarela SIP de la PBX

1. En OMC, seleccione la pestaña **Líneas externas** > **SIP** > **Pasarelas SIP** > **Detalles de parámetros de pasarelas** >**Seguridad**
2. Revise/modifique los siguientes campos:

SRTP	Seleccione **Habilitado**: el cifrado SRTP se activará en la pasarela SIP de la PBX. Valor predeterminado: **Deshabilitado** (el cifrado SRTP estará desactivado en la pasarela SIP de la PBX). **SRTP** solo se puede configurar si **SIP-TLS** está habilitado en la pasarela SIP de la PBX (véase: Activación y configuración de SIP-TLS en la pasarela SIP de la PBX *(en la página 37)*). Si **SRTP** está habilitado, OMC indica que las siguientes funciones no son compatibles y deben deshabilitarse: • RTP Directo • Transferencia de códecs para enlaces SIP • Códec G722, G729 • Códec OPUS • Modo fax T.38 Al hacer clic en **Aceptar** para confirmar la activación de SRTP, se realiza automáticamente lo siguiente en la pestaña **Medios**: • El campo **RTP Directo** se deshabilita, desactivando así la transferencia de códecs para enlaces SIP automáticamente • Si el **modo Fax** es **T38**, se establece en **G711** y se atenúa. • El códec **G722**se elimina de la lista desplegable **Códec/estructura de tramas forzados**. Si ya se ha seleccionado el códec **G722**, se establece en **Ninguno**. • El códec **G722** se elimina de las listas **Códecs disponibles** y **Códecs seleccionados**. • El códec **OPUS**se elimina de la lista desplegable **Códec/estructura de tramas forzados**. Si ya se ha seleccionado el códec OPUS, se establece en **Ninguno**. • El códec **OPUS** se elimina de las listas **Códecs disponibles** y **Códecs seleccionados**. NOTA: cuando **SRTP** está deshabilitado, **RTP Directo** y otros campos correspondientes se establecen en sus valores por defecto.

Atributo de vida útil de la clave en SDP	• **Habilitado**: se añade un valor de vida útil de la clave a la oferta de SDP. • **Deshabilitado** (opción predeterminada): no se añade ningún valor de vida útil de la clave a la oferta de SDP. La vida útil de la clave es ilimitada. Este campo solo se puede configurar cuando **SRTP** está habilitado. Si **SRTP** no está habilitado, esta casilla aparece deshabilitada y atenuada.
Conjuntos criptográficos	
Conjuntos disponibles/Conjuntos seleccionados	Estas áreas se emplean para seleccionar la lista de conjuntos criptográficos que pueden ser utilizados por la PBX. La lista **Conjuntos seleccionados** se crea a partir de la lista **Conjuntos disponibles**, utilizando las flechas laterales (==>,<==). La prioridad de cada conjunto en la lista puede gestionarse con los botones **Arriba**/**Abajo** (la prioridad máxima está en la parte superior de la lista). Por defecto, todos los conjuntos están seleccionados. Este campo solo se puede configurar cuando **SRTP** está habilitado.

3. Haga clic en **OK** para validar

Capítulo 5

Autenticación e integridad del software de la PBX

5.1. Introducción

Hasta la versión R4.0, las versiones de software de OXO Connect Evolution se publican sin autenticación.

A partir de la versión R5.0, para superar estas amenazas, el software de OXO Connect Evolution incluye un mecanismo que:

- Autentifica el software: garantiza que el software ha sido entregado por Alcatel-Lucent Enterprise.
- Garantiza la integridad del software: garantiza que el software no se ha modificado ni corrompido, y que es conforme a su entrega original.

5.2. Servicios ofrecidos

Esta función proporciona las siguientes protecciones contra la instalación de software corrupto:

- Garantiza que un software con versión R.5.0 o superior, que se instala en una PBX, se emite por Alcatel-Lucent Enterprise, y que no se ha modificado de ninguna manera respecto al facilitado por Alcatel-Lucent Enterprise:
  - En el caso de una instalación de software a través de LoLa o USB, un fallo de autenticación y comprobación de la integridad del software aborta la instalación del software, y la PBX se reinicia en el software que se estaba ejecutando anteriormente, en su caso.
  - En el caso de una actualización de software de la versión R4.0 o inferior a R5.0 o superior, la autenticación y la comprobación de la integridad del software evitan que se ejecute un software corrupto, retrocediendo al software instalado anteriormente.
  - La actualización de software a través de Cloud Connect admite el mismo nivel de autenticación y comprobación de integridad que la actualización de software a través de OMC.
- Mediante un control periódico, la PBX comprueba e indica si el software está dañado. Si es el caso, la PBX sigue funcionando, pero se genera un evento para informar de que el software está dañado.

Esto garantiza que en una versión R5.0 o superior de la PBX, solo se ejecuta el software de Alcatel-Lucent Enterprise, y que ningún software, script o componente adicional se ejecuta en paralelo.

5.3. Proceso de autenticación y comprobación de la integridad

La autenticación e integridad del software se comprueba gracias a una firma digital. La firma permite verificar que Alcatel-Lucent Enterpriseha emitido el software, y una suma de comprobación (hash) permite verificar que no ha sido modificado o que no está dañado.

El proceso de firma se basa en una criptografía de claves asimétrica, que utiliza dos claves diferentes:

- Una clave privada, mantenida en secreto, que se utiliza para la firma binaria
- Una clave pública para verificar la firma

  La clave pública puede ser distribuida sin restricciones, pero no debe modificarse.

Capítulo 5 *Autenticación e integridad del software de la PBX*

El proceso para generar una firma digital es el siguiente:

- Cálculo del código hash de los binarios
- Firma del código hash que utiliza la clave privada

> **Nota:**
> Los algoritmos utilizados para el hashing y la firma son:
> - Para el algoritmo de hashing: SHA-2 (256 bits)
> - Para el algoritmo de firma: RSA2048

Al comprobar el binario, el software de la PBX:

- comprueba la firma del código hash. Garantiza el origen de la firma, ya que solo la clave pública puede validar la firma generada con la correspondiente clave privada.
- Calcula un hash de los binarios y lo compara con el firmado. Si es igual, el software queda autenticado y no es corrupto. Si es diferente, el software es corrupto.

5.4. Funcionamiento

5.4.1. Actualización del software de la PBX de la versión R4.0 o inferior a R5.0 o superior

La PBX que ejecuta un software R4.0 o inferior no puede comprobar la autenticidad e integridad del software R5.0 que se está cargando: el procedimiento de carga lo acepta.

La PBX comprueba la autenticidad y la integridad tras el reinicio y cambia al nuevo software R5.0 (o superior). Comprueba que Alcatel-Lucent Enterprise ha emitido la firma, y que el hash confirma que los binarios no son corruptos.

Si la operación tiene éxito, el nuevo software se ejecuta en la PBX, y se puede realizar una restauración de los datos del cliente.

Si la autenticación o la comprobación de integridad fallan, la PBX vuelve al software inicial. El registro de restablecimiento se actualiza con el fallo de la firma a causa del retroceso del software. El software corrupto permanece almacenado en la PBX para permitir un análisis posterior, según el mecanismo de migración existente en la PBX.

> **Nota:**
> La actualización de la PBX a un software R5.0 sin firmar falla. En este caso, la instalación del software se realiza con éxito, pero cuando la PBX se reinicia con este software R5.0 sin firmar, la comprobación de la firma falla y la PBX vuelve al software inicial.

5.4.2. Actualización del software de la PBX de R5.0 Vx a R5.0 Vx+n

El software R5.0 Vx puede comprobar la autenticidad e integridad del software que se carga.

Tras la carga, la PBX comprueba su autenticidad e integridad:

- En caso de fallo, se rechaza la actualización del software y se genera un evento para informar de que el software estaba dañado.
- Si es correcto, entonces se activa un reinicio y un intercambio.

Nota:
La actualización a un software R5.0 Vx+n sin firmar falla.

5.4.3. Cambiar el software de la PBX a una versión anterior de R5.0 o superior a R4.0 o inferior

El software R5.0 (o superior) autoriza el cambio a una versión anterior como R4.0 o inferior mediante OMC.

Aviso:
Después de cambiar el software a una versión anterior, no habrá más verificación del software (autenticidad e integridad), porque el software instalado es un software no firmado.

5.4.4. Instalación del software R5.0 o superior a través de LoLa o un lápiz USB

Durante la instalación del software, la PBX comprueba la autenticidad y la integridad del software, y aborta la instalación en caso de que falle la comprobación de la firma:

- se muestra un mensaje de advertencia en la aplicación LoLa, o en el registro de la consola (para la instalación a través del lápiz USB).
- La PBX se reinicia con el software y la configuración actuales.

Nota:
La instalación de un software R5.0 sin firmar falla a través de una LoLa o un lápiz USB.

5.4.5. Control periódico del software

La PBX realiza una comprobación de la autenticación del software una vez a la semana, cada domingo a medianoche.

En caso de fallo:

- Se genera un evento y se muestra en la **tabla de historial** de OMC (`R_BINARY_SIGNATURE_FAILURE`). Véase el documento [12] para obtener más información.
- La PBX sigue funcionando.

Para solucionar el problema, se recomienda actualizar la PBX a una versión de software válida.

Capítulo 6

Gestión de certificados

6.1. Introducción

El acceso al servidor de llamadas se establece a través de una conexión HTTPS. Durante el establecimiento de la conexión, el servidor se autentica con un certificado (autenticación del servidor). Algunos clientes también deben autenticarse con un certificado (autenticación mutua).

La PCX admite la autenticación mediante servidor con otros terminales SIP.

OMC puede comprobar la validez del certificado del servidor para las conexiones HTTPS. El usuario puede deshabilitar esta comprobación.

Los siguientes certificados están instalados de forma predeterminada en OXO Connect Evolution:

- El certificado “Alcatel-Lucent Enterprise Solutions” CA
- El certificado “Alcatel-Lucent Enterprise Wired Phones” subCA
- Un certificado autofirmado (y su clave privada asociada), que es la misma en todos los sistemas, con el CN "alize". Este certificado se llama el **certificado estático** en este documento
- Un certificado de la autoridad certificadora local, usado para firmar el certificado dinámico (la “CA local”)
- Un certificado generado (y su clave privada asociada), diferente para cada OXO Connect Evolution, usado para la autenticación por todos los clientes, en la LAN y en la WAN. Este certificado se llama el **certificado dinámico** en este documento
- Certificados almacenados en el Trust Store (almacén de confianza), que son utilizados por algunas aplicaciones para identificar los servidores externos.
- Un certificado estático para la autenticación del punto de acceso de HAN
- Cadena CA para autenticación ALE-2 DeskPhone/ALE-3 DeskPhone

A partir de R6.0, se puede utilizar un **certificado de servidor público** para:

- Conexión SIP TLS pública
- Conexiones HTTPS a OXO Connect Evolution desde Internet

El **certificado de servidor público** no está instalado de forma predeterminada. Para obtener más información, consulte Certificado de servidor público *(en la página 50)*.

Los certificados CA y sub-CA se utilizan para identificar a los clientes mediante sus certificados, cuando estos certificados del cliente están firmados por el PKI de Alcatel-Lucent Enterprise.

El **certificado estático**, el **certificado dinámico** y el **certificado de servidor público** son certificados de servidor que los clientes utilizan para identificar OXO Connect Evolution.

Los certificados en el Trust Store se utilizan para identificar a los servidores cuando OXO Connect Evolution se utiliza como cliente.

Capítulo 6 *Gestión de certificados*

La tabla siguiente detalla qué certificado se presenta al cliente de acuerdo con el número de puerto utilizado. El número de puerto utilizado depende del tipo de cliente y el tipo de acceso (local o remoto). Para obtener más información, consulte Control de acceso por abonado y aplicación *(en la página 75)*.

Tabla 6-1 Certificado presentado al cliente

Número puerto	Certificado presentado al cliente
443	Cadena de certificado dinámico
10443	Certificado estático
11443	Certificado estático de HAP
50443	Cadena de certificado dinámico certificado público del servidor, si existe

La cadena de certificado dinámico es el certificado dinámico seguido de la CA local.

Es posible instalar certificados personalizados en OXO Connect Evolution, utilizados en lugar de los certificados firmados por la CA local. Significa que los certificados de servidor de OXO Connect Evolution pueden ser firmados por cualquier autoridad de certificación y pueden ser aceptados automáticamente por los navegadores más populares.

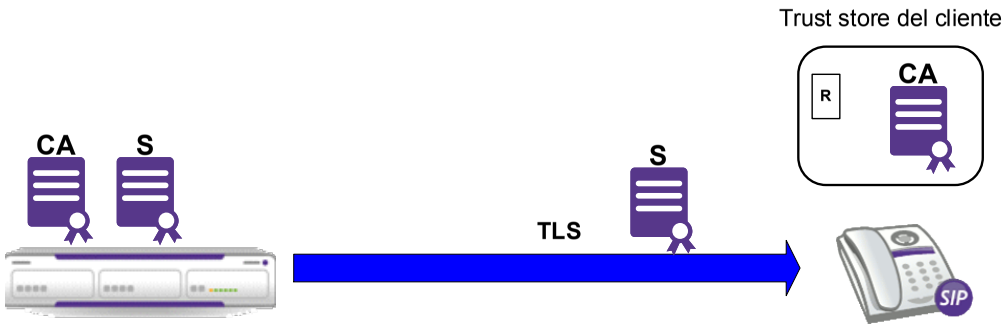
Para ser aceptado por los clientes como un certificado válido, los certificados de servidor deben ser aceptados, lo que implica que debe instalarse el certificado de la CA local en el almacén de confianza del cliente. Si el certificado no se reconoce como válido, el cliente muestra una advertencia para indicar que el servidor no es de confianza y, por lo tanto, no es seguro.

6.1.1. Autenticación mediante servidor

En el caso de la autenticación mediante servidor, el PCX se autentica mediante el certificado que ha proporcionado al cliente.

Si la función de conexión HTTPS está habilitada, OMC requiere el certificado de OXO Connect Evolution.

Para utilizar esta función, debe instalarse Internet Explorer 8 o posterior en el cliente.



S: certificado dinámico firmado por la CA
CA (autoridad de certificación local)

Figura 6-1 Certificado dinámico: el certificado del servidor es firmado por el certificado de la CA local.

En este caso, para establecer una conexión sin advertencia de seguridad, el certificado de la CA local debe instalarse en el almacén de confianza del cliente.

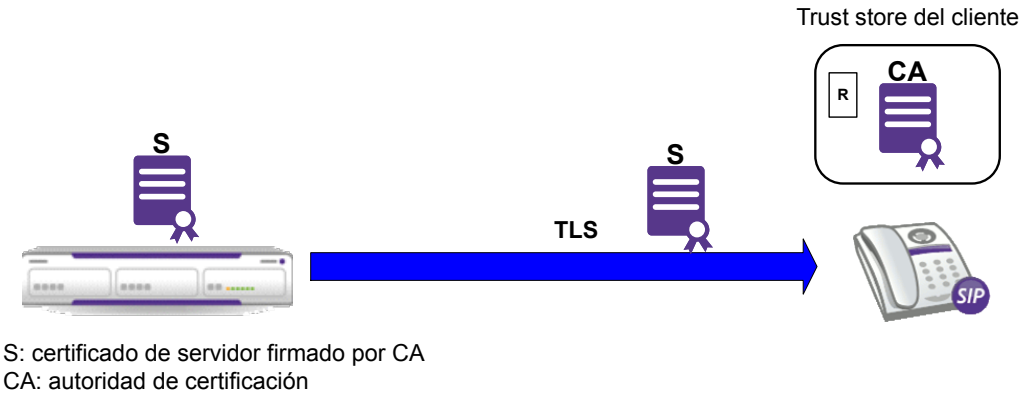


Figura 6-2 Certificado personalizado: el certificado del servidor es firmado por una CA.

En este escenario, es la autoridad certificadora (CA) que firmó el certificado del servidor, que debe estar instalado en el almacén de confianza del cliente.

La autoridad de certificación de entidades reconocidas (Verisign, Thawte, etc.). ya está instalada en los navegadores más populares (Firefox, Internet Explorer, Chrome). Si la CA no está ya instalada en el almacén de confianza, debe hacerse antes de la conexión al servidor para evitar advertencias de seguridad.

6.2. Accesos lógicos del sistema

Puede accederse a OXO Connect Evolution usando diferentes nombres.

Los diferentes accesos lógicos al sistema son:

- La dirección IP de la VLAN de datos
- La dirección IP de la VLAN de voz
- La dirección IP de gestión
- La dirección IP externa (en la WAN)
- El nombre “alize” si el sistema es el propio servidor DNS
- El nombre de host de OXO Connect Evolution (configurado o recuperado mediante DHCP).
- Direcciones IP para conexiones de módem

Todos estos parámetros (llamados “nombres”) deben incluirse en el certificado del servidor para obtener conexiones sin advertencias. Se incluyen automáticamente en el certificado dinámico y en el CSR utilizado para generar el certificado personalizado.

Importante:

Un certificado habilita los accesos correspondientes a los nombres que contiene.

Si se cambian los accesos (dirección IP de la WAN, direcciones IP de la LAN, etc.) debe generarse un nuevo certificado e instalarse en OXO Connect Evolution y en los clientes que se conectan a OXO Connect Evolution.

Capítulo 6 *Gestión de certificados*

6.3. Certificado dinámico

El certificado de la CA local utilizado para firmar el certificado dinámico tiene las siguientes características:

- Certificado CA raíz
- Algoritmo de firma: sha256WithRSAEncryption
- Nombre común: OXO Root CA + número de serie
- Validez: 3650 días
- Longitud de la clave: 2048 bits

El certificado dinámico tiene las siguientes características:

- Firmado por una autoridad (la CA local)
- Algoritmo de firma: sha256WithRSAEncryption
- Nombre común: nombre de host configurado en OMC: **Hardware y límites > Configuración de LAN/IP**
- Validez: 3650 días
- Longitud de la clave: 2048 bits
- Nombres alternativos del asunto:
  - Nombre local
  - Dirección IP de los datos Eth0
  - Dirección IP de la voz Eth0
  - Dirección IP de Eth1
  - **Dirección IP de gestión**
  - **Dirección IP del router/nombre de dominio** (dirección IP pública/FQDN para conectarse a OXO Connect Evolution desde Internet)

El CN (nombre común) y los nombres de asunto alternativo tienen una función importante en las conexiones seguras: se utilizan para comprobar la coincidencia entre la URL usada para acceder a OXO Connect Evolution y el certificado que se presenta al cliente. Si el certificado y la URL no coinciden, el cliente normalmente muestra una advertencia para indicar un riesgo de seguridad con la conexión en curso.

El CN (nombre común) del certificado dinámico es el nombre configurado en OMC: **Hardware y límites > Configuración de LAN/IP**, que permite acceder a OXO Connect Evolution con la URL https://[nombre local] en la LAN sin avisar.

El certificado contiene algunos nombres alternativos (función estándar de los certificados X509v3) que permite acceder a OXO Connect Evolution mediante su dirección IP, su nombre de host, la dirección del enrutador externo o su dirección IP de gestión, sin advertencias.

Una vez creado, el certificado dinámico es válido durante 10 años. Después de este tiempo, el certificado se considera “caducado”, que es otra razón para ver una advertencia en cada conexión.

Para librarse de las advertencias, debe generarse otro certificado. Para obtener más información, consulte Generar un nuevo certificado dinámico *(en la página 56)*.

Capítulo 6 Gestión de certificados

A partir de OXO Connect Evolution R3.2, la PBX realiza un reinicio automático en caliente cuando su certificado dinámico actual es reemplazado o regenerado (véase: Generar un nuevo certificado dinámico *(en la página 56)*).

6.3.1. Regeneración automática del certificado dinámico

El certificado dinámico se regenera solo cuando no existe todavía o cuando alguna información almacenada en el certificado ya no es válida. Dicha información es la dirección IP de OXO Connect Evolution, el nombre (dirección) del enrutador de acceso externo y la dirección IP de gestión.

El certificado CA local, su clave privada, el certificado dinámico y la clave privada se almacenan en un almacenamiento persistente de OXO Connect Evolution. Como consecuencia, si después de una migración se restaura la configuración de la red a como estaba durante la creación del certificado, el certificado no cambia y no es necesario reinstalarlo.

Si se cambia la tarjeta CPU, se genera un nuevo juego de certificados y debe reinstalarse la CA local en todos los clientes.

Como los certificados del servidor en un solo OXO Connect Evolution son siempre firmados por la misma CA local (excepto cuando se ha cambiado la tarjeta CPU o se ha regenerado la CA mediante la herramienta web), los nuevos certificados del servidor generados son siempre aceptados por los clientes que tienen la CA local instalada en su almacén de confianza. Por este motivo, los clientes deben instalar el certificado CA local en su almacén de confianza y no el propio certificado del servidor.

La tabla siguiente muestra los eventos que activan la regeneración del certificado.

Tabla 6-2 Regeneración automática del certificado

Evento	Regeneración auto-mática del certificado
Restablecimiento en frío/caliente	
LoLa Instalación LoLa	
Cambio de IP@	Sí
Cambio de nombre de host	Sí
Cambio de IP@ de gestión	Sí
Cambio de nombre de acceso del enrutador	Sí
No hay certificado en el momento del arranque	Sí (**)

(**) Si el certificado no está firmado por la CA local actual, también se regenera.

6.4. Certificado de servidor público

El **certificado de servidor público** se utiliza para los siguientes fines:

- Conexión SIP TLS pública
- Conexiones HTTPS a OXO Connect Evolution desde Internet

Por defecto, el **certificado de servidor público** no está presente en OXO Connect Evolution.

Capítulo 6 Gestión de certificados

El **certificado de servidor público** está disponible tras importarlo a través de la herramienta basada en Web. Puede ser:

- Un certificado de servidor público firmado por una CA externa con CSR generado desde OXO Connect Evolution a través de la herramienta basada en Web
- Un certificado de servidor público firmado por una CA externa

El procedimiento para importar el **certificado de servidor público** se detalla en la sección Implementación de un certificado personalizado *(en la página 62)*.

Nota:
Hasta que se instale un certificado de servidor público, el certificado de servidor LAN existente se utiliza para SIP TLS público y conexiones a través de WAN.

El certificado de servidor público tiene las siguientes características:

- CN: **Dirección IP del router/nombre de dominio** (dirección IP pública/FQDN para conectarse a OXO Connect Evolution desde Internet)
- SAN: **Dirección IP del router/nombre de dominio** (dirección IP pública/FQDN para conectarse a OXO Connect Evolution desde Internet)

6.5. Certificados personalizados

Es posible instalar certificados personalizados en OXO Connect Evolution, utilizados en lugar de los certificados firmados por la CA local. Significa que los certificados de servidor de OXO Connect Evolution pueden ser firmados por cualquier autoridad de certificación y pueden ser aceptados automáticamente por los navegadores más populares.

El archivo generado por la CA puede ser de distintos tipos. El uso del archivo CSR generado por OXO Connect Evolution es opcional.

El CSR es un archivo PKCS#10 en formato PEM. Este archivo contiene información sobre OXO Connect Evolution que se insertará en el certificado del servidor final. La clave privada no está incluida en el CSR.

- Cuando se utiliza el CSR, el archivo firmado por la CA puede ser:
  - Un archivo PKCS#7 en formato PEM. Debe contener al menos el certificado del servidor, pero puede contener otros objetos, como el certificado CA.
  - Un archivo de certificado simple en formato PEM

  Cuando se usa el CSR, la CA no genera una clave privada. Se utiliza la clave privada generada por OXO Connect Evolution.
- Cuando no se utiliza el CSR, el archivo firmado por la CA es
  - Un archivo PKCS#12 (que contiene el certificado del servidor y la clave privada). El archivo está en formato binario
  - Dos archivos separados para el certificado y la clave privada (no integrados en un archivo PKCS#12)

  Cuando no se usa el CSR, la CA genera una nueva clave privada/pareja de certificados. No se utiliza la clave privada generada por OXO Connect Evolution.

Las secciones siguientes describen el procedimiento para implantar el certificado en ambos casos.

6.5.1. Certificado del servidor y clave privada

Cuando se importa una cadena de certificados a OXO Connect Evolution a través de la herramienta basada en Web, se extrae el contenido de la cadena (certificado del servidor, CA raíz, CA(s) intermedia(s), clave privada).

La clave privada se almacena en una zona de almacenamiento seguro del sistema. Queda protegida en caso de restablecimiento o reinstalación del sistema.

El certificado del servidor, la CA raíz y la(s) CA intermedia(s) se almacenan en la memoria flash del sistema. Se conservan en caso de restablecimiento o reinstalación del sistema.

Cuando se genera un CSR, la clave privada correspondiente (la “clave privada alternativa”) se genera también y debe conservarse mientras se lleva a cabo el proceso de firma.

La clave privada alternativa se almacena en el sistema, lista para ser instalada junto con el certificado firmado.

En esta fase, el certificado del servidor y la clave privada no cambian. La clave privada alternativa se almacena en el sistema, segura contra restablecimiento o reinstalación.

Cuando se instala un certificado firmado (archivo pem o archivo PKCS#7), el certificado actual es sustituido por el nuevo certificado recibido y la clave privada actual es sustituida por la clave alternativa.

Cuando se instala un archivo PKCS#12, el certificado actual y la clave privada se eliminan y sustituyen por los extraídos del archivo PKCS#12. No se usa la clave privada alternativa.

Cuando se instala el certificado y la clave privada mediante dos archivos separados en formato pem, el certificado actual y la clave privada se eliminan y sustituyen por los recibidos en los dos archivos.

Capítulo 6 Gestión de certificados

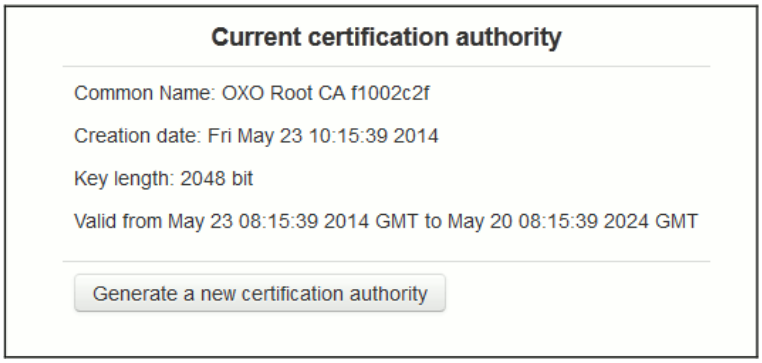
6.6. Autoridad de certificación local

6.6.1. Mostrar la información de la autoridad certificadora

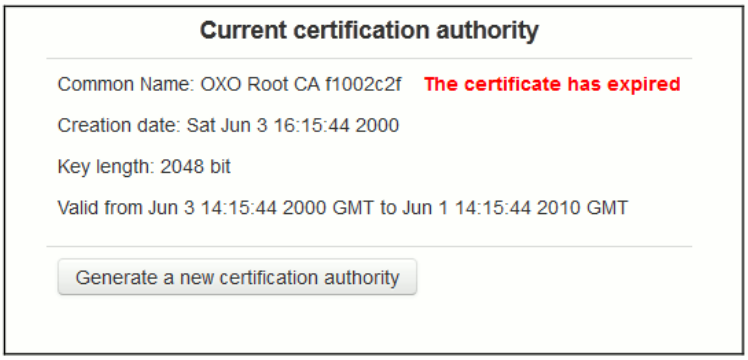
Para mostrar la información de la autoridad certificadora:

1. Abra una sesión en la herramienta web como instalador
2. Seleccione **Certificates** > **Certification Authority**

   El panel **Current certificate authority** facilita alguna información sobre la CA local: nombre común, fecha de creación, longitud de la clave y fechas de validez.



   Si la CA ha caducado, la información se muestra en rojo, como se muestra a continuación:



6.6.2. Generar un nuevo certificado CA local

Para generar un nuevo certificado CA local:

1. Abra una sesión en la herramienta web como instalador
2. Seleccione **Certificates** > **Certification Authority**
3. En el panel **Current certificate authority**, haga clic en **Generate a new certification authority**
4. Se abre una ventana emergente que advierte de que se perderán el certificado actual y la clave privada. Haga clic en **OK**

6.7. Gestión del certificado de acceso local

Capítulo 6 *Gestión de certificados*

6.7.1. Requisitos previos

La configuración de red de OXO Connect Evolution debe completarse antes de comenzar el procedimiento de certificación.

Los siguientes parámetros no deben modificarse después de haber comenzado el procedimiento:

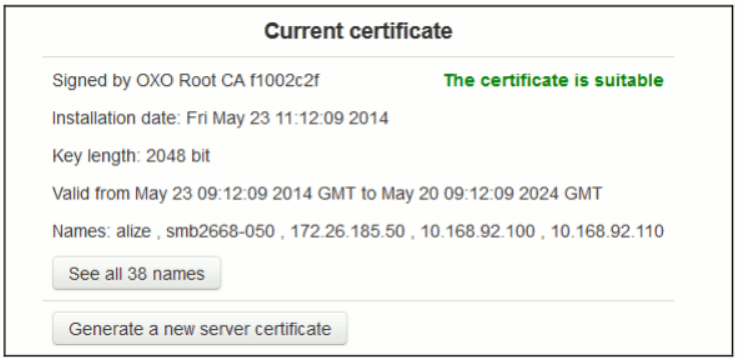
- Dirección IP de los datos Eth0
- Dirección IP de la voz Eth0
- Dirección IP de Eth1
- Dirección IP de gestión
- Dirección IP de la WAN

6.7.2. Mostrar la información del certificado actual

Para mostrar la información del certificado actual:

1. Abra una sesión en la herramienta web como instalador
2. Seleccione **Certificates** > **Server certificate**

   El panel **Current certificate** facilita alguna información sobre el certificado del servidor actual del sistema (la fecha de instalación, su estado de firma, el tamaño de su clave, sus fechas de validez y sus nombres).



Si el certificado no es válido porque ha caducado el periodo de validez o porque falta al menos un nombre, la información se muestra en rojo como se muestra a continuación:

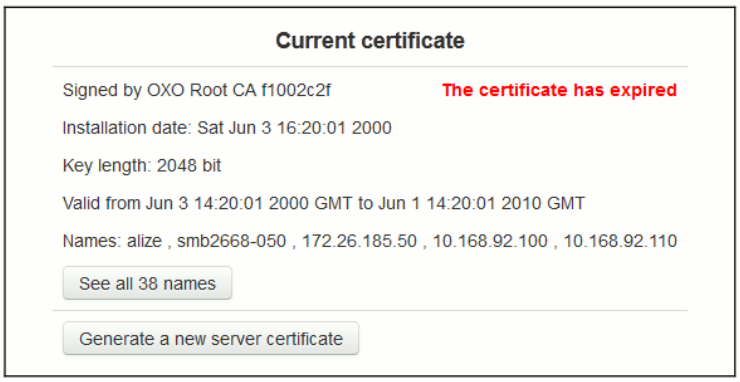


Figura 6-3 Información del certificado caducada

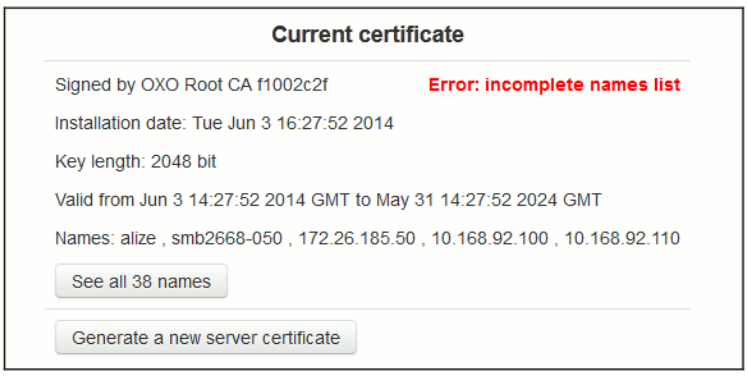
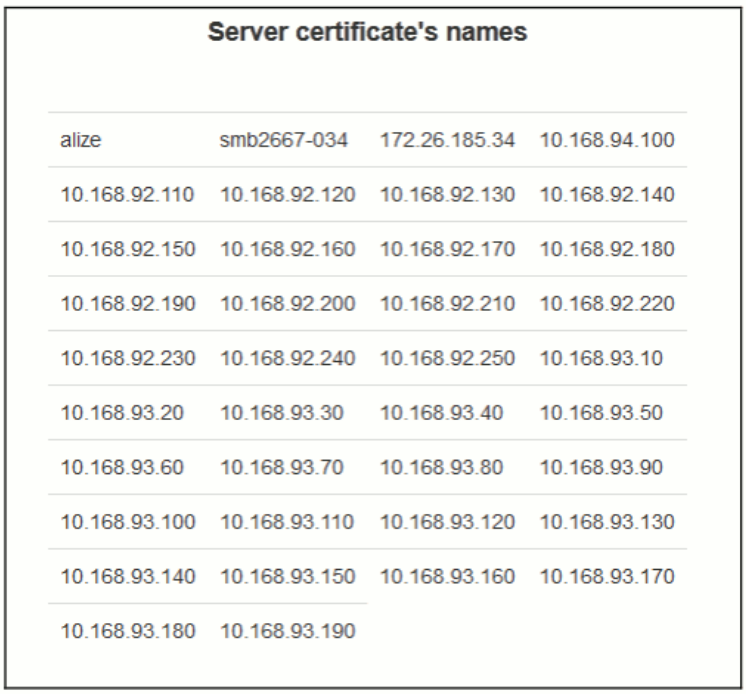


Figura 6-4 Información de lista de nombres incompleta

Nota:
Cuando el certificado es considerado no válido por OXO Connect Evolution, no significa que un cliente mostrará una advertencia: las fechas de validez no siempre son comprobadas por los clientes y un nombre ausente solo activa una advertencia si se utiliza este nombre para acceder a OXO Connect Evolution.

3. Se muestran hasta 5 nombres en esta pantalla. Haga clic en el botón **See all [number of names] names** para mostrar la lista completa si el certificado incluye más de cinco nombres.



6.7.3. Generar un nuevo certificado dinámico

Cuando el certificado dinámico actual haya caducado o si la lista de nombres está incompleta, debe regenerarse.

Atención:
No debe utilizarse el procedimiento siguiente cuando se utiliza un certificado personalizado firmado por una CA. Si lo hace, se eliminará el certificado firmado.

Para generar un nuevo certificado dinámico:

1. Abra una sesión en la herramienta web como instalador
2. Seleccione **Certificates** > **Server certificate**
3. Haga clic en **Generate a new server certificate**

   Se muestra un mensaje de advertencia que indica que es necesario reiniciar OXO Connect Evolution (reinicio en caliente).

4. Haga clic en **OK** para validar la acción.

   Se muestra un mensaje de advertencia adicional que indica que el certificado actual y la clave privada se perderán después de reiniciar

5. Haga clic en **OK** para validar la acción.

   OXO Connect Evolution se reinicia con el certificado dinámico generado nuevo.

6.7.4. Implementación de un certificado personalizado

6.7.4.1. Implantación del certificado cuando se usa el CSR

1. El instalador utiliza OXO Connect Evolution para generar un CSR: consulte Generar un archivo CSR y clave privada *(en la página 58)*
2. El instalador envía el CSR a una autoridad certificadora
3. La CA genera un certificado firmado
4. El certificado se envía al cliente (o al instalador)
5. El certificado firmado se instala en OXO Connect Evolution: consulte Instalar un certificado personalizado *(en la página 60)*
6. El certificado CA se instala en los clientes: consulte Implementación del certificado del servidor en los clientes *(en la página 68)*

Este procedimiento es especialmente seguro, porque la clave privada generada por OXO Connect Evolution nunca se extrae de su ubicación en el sistema.

En función de la CA, puede ser necesario aportar algunos datos sobre el certificado futuro (nombres que se incluirán y fechas de validez). Esta información ya se incluye en el CSR, y se muestra en la herramienta utilizada para generarlo

6.7.4.2. Implantación del certificado cuando no se usa el CSR

1. El cliente envía una solicitud a la autoridad certificadora con la siguiente información sobre la empresa y su servidor:
   - El nombre común del certificado: puede ser cualquier cosa, por ejemplo el nombre de host de OXO Connect Evolution
   - Los nombres alternativos: todos los accesos, diferentes del nombre común, que pueden utilizarse para acceder a OXO Connect Evolution:
     - Dirección IP de los datos Eth0
     - Dirección IP de la voz Eth0
     - Dirección IP de Eth1
     - **Dirección IP de gestión**
     - Dirección IP de la WAN
     - Dirección IP de gestión

     Nota:
     Si uno de los nombres alternativos no se encuentra en el certificado, se generará una advertencia en cada conexión usando este nombre.
   - Las fechas de validez del certificado o la duración del certificado
   - El tamaño de las claves RSA (se recomiendan claves de 2048 bits)
2. La CA facilita:
   - Un archivo PKCS#12 cifrado que contiene el certificado del servidor, el certificado CA y la clave privada del servidor.
   - Archivos separados para el certificado y la clave privada (no integrados en un archivo PKCS#12). En tal caso, solo la clave privada está cifrada.
3. El PKCS#12 o los archivos separados (certificado y clave privada) se envían al instalador
4. El instalador pone el certificado del servidor y la clave en OXO Connect Evolution: consulte Instalar un certificado personalizado *(en la página 60)*
5. El certificado CA se instala en los clientes: consulte Implementación del certificado del servidor en los clientes *(en la página 68)*

6.7.4.3. Generar un archivo CSR y clave privada

A continuación se describe cómo generar un archivo CSR y una clave privada cuando se necesita un CSR para generar un certificado personalizado.

Para generar un archivo CSR y una clave privada asociada:

1. Abra una sesión en la herramienta web como instalador
2. Seleccione **Certificates** > **Server certificate**

   El panel **Generate a Certificate Signing Request and a private key** muestra información sobre el certificado futuro (nombres y tamaño de las claves).

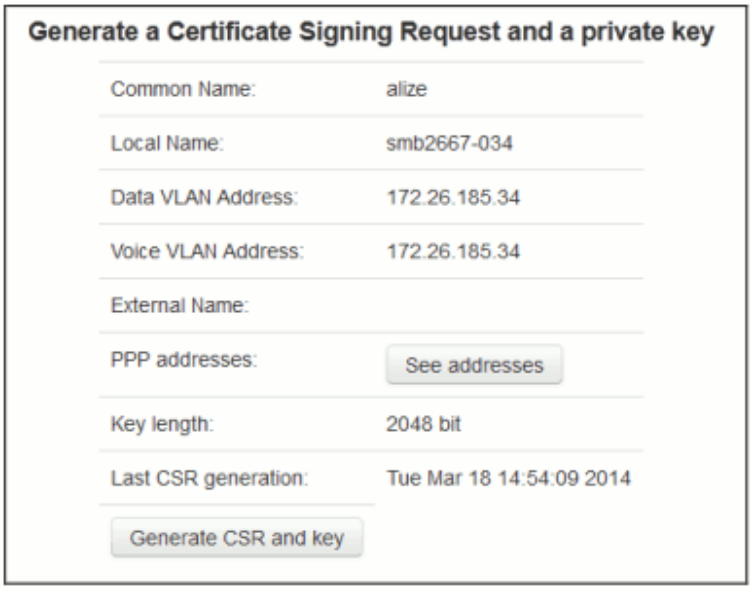
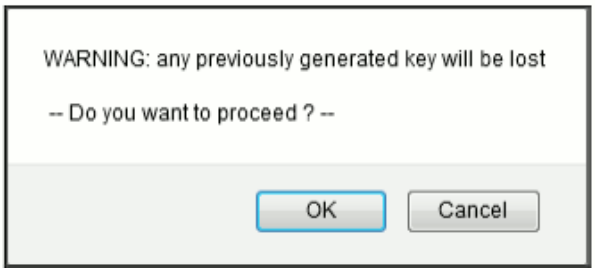


Figura 6-5 Panel **Generate a Certificate Signing Request and a private key**

3. Haga clic en el icono **Generate CSR and key**

   Se abre una ventana emergente que advierte de que se perderá la clave generada previamente.



4. Haga clic en **OK**

   Esto fuerza la generación de una clave privada y de un CSR.

   La clave privada se almacena en la memoria flash del sistema pero no se utiliza en esta etapa. Esta clave se llama **clave privada alternativa** en este documento.

   El CSR incluye todos los nombres mostrados en el panel **Generate a Certificate Signing Request and a private key**. Es responsabilidad del PKI que utilizará el CSR para incluir todos estos nombres en el certificado.

5. En la ventana emergente que se abre, explore para seleccionar una ubicación donde guardar el archivo CSR

6.7.4.4. Instalar un certificado personalizado

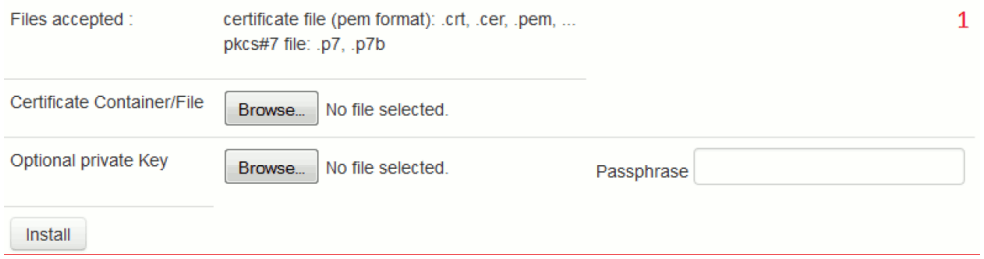
A continuación, se describe cómo instalar un certificado personalizado firmado por una CA en OXO Connect Evolution.

1. Abra una sesión en la herramienta web como instalador
2. Seleccione **Certificates** > **Server certificate**

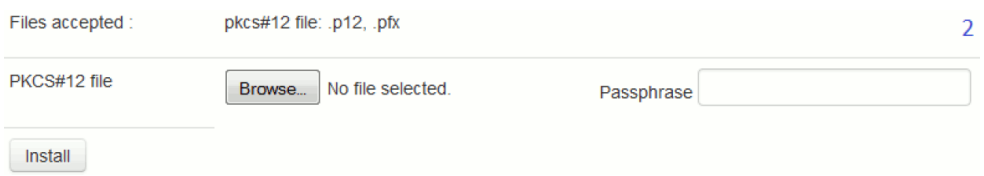
   En la ventana que se muestra, el tercer panel **Install a certificate** permite instalar un certificado personalizado.
3. En función del tipo de certificado:
   - Para instalar un certificado en formato pem o un archivo PKCS#7
     - Haga clic en **Browse** y seleccione los archivos PKCS#7 o pem
     - Si se facilita una clave privada, haga clic en **Browse** para seleccionar la clave privada e introduzca la **Passphrase** si la clave privada está cifrada.

       Nota:
       Si no se facilita ninguna clave privada, se asume que ha sido creada en la memoria flash del sistema mediante la acción “Generate CSR and key”.

     - Haga clic en **Install**



   - Para instalar un archivo PKCS#12:
     - Haga clic en **Browse** y seleccione el archivo PKCS#12 que contiene el certificado y la clave privada
     - Si la clave privada está cifrada, introduzca el valor **Passphrase**
     - Haga clic en **Install**



Después de la instalación, se restablece la conexión con el sistema y se pierde la conexión con la herramienta web.

En caso de que el certificado y la clave privada facilitados no coincidan, el certificado no se instala y el certificado actual se mantiene intacto.

6.8. Gestión del certificado de servidor público

6.8.1. Requisitos previos

La configuración de red de OXO Connect Evolution debe completarse antes de comenzar el procedimiento de certificación.

Los siguientes parámetros no deben modificarse después de haber comenzado el procedimiento:

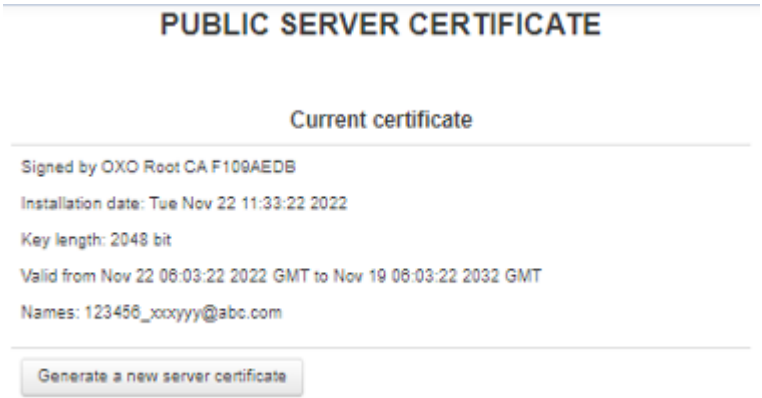
- **Dirección IP del router/nombre de dominio** (dirección IP pública/FQDN para conectarse a OXO Connect Evolution desde Internet)

6.8.2. Mostrar la información del certificado actual

Para mostrar la información del certificado actual:

1. Abra una sesión en la herramienta web como instalador
2. Seleccione **Certificates > Public Server certificate**

   El panel **Current certificate** facilita alguna información sobre el certificado de servidor actual del sistema (la fecha de instalación, su estado de firma, el tamaño de su clave, sus fechas de validez y sus nombres).



   Si el certificado no es válido porque ha vencido el período de validez o porque falta al menos un nombre, la información aparece en color en rojo.

6.8.3. Implementación de un certificado personalizado

6.8.3.1. Implantación del certificado cuando se usa el CSR

1. El instalador utiliza OXO Connect Evolution para generar un CSR: consulte Generar un archivo CSR y clave privada *(en la página 62)*
2. El instalador envía el CSR a una autoridad certificadora
3. La CA genera un certificado firmado
4. El certificado se envía al cliente (o al instalador)
5. El certificado firmado se instala en OXO Connect Evolution: consulte Instalar un certificado personalizado *(en la página 64)*
6. El certificado CA se instala en los clientes: consulte Implementación del certificado del servidor en los clientes *(en la página 68)*

Este procedimiento es especialmente seguro, porque la clave privada generada por OXO Connect Evolution nunca se extrae de su ubicación en el sistema.

En función de la CA, puede ser necesario aportar algunos datos sobre el certificado futuro (nombres que se incluirán y fechas de validez). Esta información ya se incluye en el CSR y aparece en la herramienta utilizada para generarlo.

6.8.3.2. Implantación del certificado cuando no se usa el CSR

1. El cliente envía una solicitud a la autoridad certificadora con la siguiente información sobre la empresa y su servidor:
   - El nombre común del certificado: **Dirección IP del router/nombre de dominio** (dirección IP pública/FQDN para conectarse a OXO Connect Evolution desde Internet)
   - Los nombres alternativos: todos los accesos, **Dirección IP del router/nombre de dominio** (dirección IP pública/FQDN para conectarse a OXO Connect Evolution desde Internet)
   - Las fechas de validez del certificado o la duración del certificado
   - El tamaño de las claves RSA (se recomiendan claves de 2048 bits)
2. La CA facilita:
   - Un archivo PKCS#12 cifrado que contiene el certificado del servidor, el certificado CA y la clave privada del servidor.
   - Archivos separados para el certificado y la clave privada (no integrados en un archivo PKCS#12). En tal caso, solo la clave privada está cifrada.
3. El PKCS#12 o los archivos separados (certificado y clave privada) se envían al instalador
4. El instalador pone el certificado del servidor y la clave en OXO Connect Evolution: consulte Instalar un certificado personalizado *(en la página 64)*
5. El certificado CA se instala en los clientes: consulte Implementación del certificado del servidor en los clientes *(en la página 68)*

6.8.3.3. Generar un archivo CSR y clave privada

A continuación se describe cómo generar un archivo CSR y una clave privada cuando se necesita un CSR para generar un certificado personalizado.

Capítulo 6 *Gestión de certificados*

Para generar un archivo CSR y una clave privada asociada:

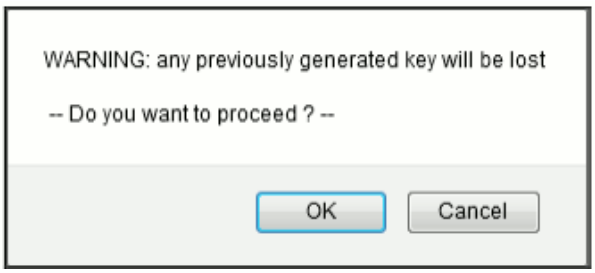
1. Abra una sesión en la herramienta web como instalador
2. Seleccione **Certificates > Public Server certificate**

   Siempre que **Dirección IP del router/nombre de dominio** esté configurado en OXO Connect Evolution, el panel **Generate a Certificate Signing Request and a private key** muestra información sobre el futuro certificado (nombres y tamaño de la clave) y el botón **Generate CSR and key** se habilita.

Figura 6-6 Panel **Generate a Certificate Signing Request and a private key**

3. Haga clic en el icono **Generate CSR and key**

   Se abre una ventana emergente que advierte de que se perderá la clave generada previamente.



4. Haga clic en **OK**

   Esto fuerza la generación de una clave privada y de un CSR.

   La clave privada se almacena en la memoria flash del sistema pero no se utiliza en esta etapa. Esta clave se llama **clave privada alternativa** en este documento.

   El CSR incluye los nombres mostrados en el panel **Generate a Certificate Signing Request and a private key**. Es responsabilidad del PKI que utilizará el CSR para incluir todos estos nombres en el certificado.

5. En la ventana emergente que se abre, explore para seleccionar una ubicación donde guardar el archivo CSR

6.8.3.4. Instalar un certificado personalizado

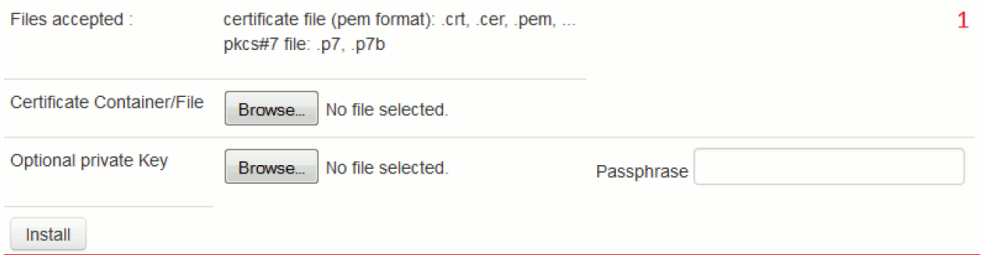
A continuación, se describe cómo instalar un certificado personalizado firmado por una CA en OXO Connect Evolution.

1. Abra una sesión en la herramienta web como instalador
2. Seleccione **Certificates > Public Server certificate**

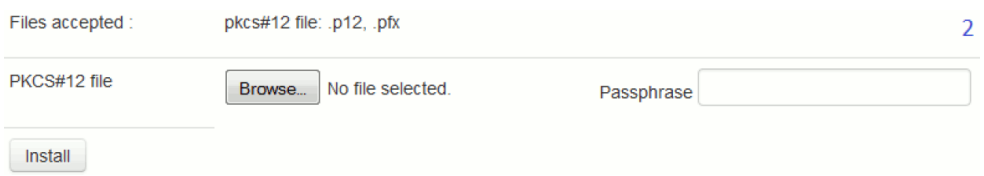
   En la ventana que se muestra, el tercer panel **Install a certificate** permite instalar un certificado personalizado.
3. En función del tipo de certificado:
   - Para instalar un certificado en formato pem o un archivo PKCS#7
     - Haga clic en **Browse** y seleccione los archivos PKCS#7 o pem
     - Si se facilita una clave privada, haga clic en **Browse** para seleccionar la clave privada e introduzca la **Passphrase** si la clave privada está cifrada.

       Nota:
       Si no se facilita ninguna clave privada, se asume que ha sido creada en la memoria flash del sistema mediante la acción “Generate CSR and key”.

     - Haga clic en **Install**



   - Para instalar un archivo PKCS#12:
     - Haga clic en **Browse** y seleccione el archivo PKCS#12 que contiene el certificado y la clave privada
     - Si la clave privada está cifrada, introduzca el valor **Passphrase**
     - Haga clic en **Install**



En caso de que el certificado y la clave privada facilitados no coincidan, el certificado no se instala y el certificado actual se mantiene intacto.

6.9. Gestionar el almacén de confianza de OXO Connect Evolution

El almacén de confianza contiene una lista de certificados públicos usados para la autenticación del servidor. Puede rellenarse con certificados adicionales del instalador.

No es posible exportar los certificados del almacén de confianza. En caso de duda sobre el contenido de un certificado, puede eliminarse y puede instalarse uno nuevo.

Los certificados en el almacén de confianza de OXO Connect Evolution están divididos en dos grupos:

- Los certificados preinstalados (incluida la autoridad de certificación del terminal ALE), que se instalan con el software OXO Connect Evolution
- Los certificados adicionales, que son instalados por el instalador

Estos dos grupos tienen sus propias políticas de gestión después de la instalación de la nueva versión de OXO Connect Evolution.

Cada grupo se muestra en una pestaña en la página **Certificates** > **Trust Store** de la herramienta basada en la web.

Se requiere un reinicio en caliente de OXO Connect Evolution cuando se añaden o eliminan autoridades de certificación del repositorio de certificados de confianza.

6.9.1. Autoridades de confianza preinstaladas

Una versión de software de OXO Connect Evolution contiene autoridades certificadoras bien conocidas disponibles en las versiones actuales de MS Windows. Estas autoridades pueden ser autoridades raíz o subCA. Se identifican mediante la versión de Internet Explorer y la fecha.

La pestaña **Pre-installed authorities** de la página **Certificates** > **Trust Store**muestra los certificados en el orden del sistema de archivos. Por cada certificado, se muestra la información siguiente: nombre común, fechas de validez y estado de validez.

No es posible añadir certificados en la pestaña **Pre-installed authorities**. Solo pueden eliminarse:

- Haga clic en el botón **Empty store**, ubicado en la parte inferior de la ventana, para eliminar todos los certificados
- Haga clic en el botón **Remove Expired Certificates**, ubicado en la parte inferior de la ventana, para eliminar todos los certificados caducados
- Haga clic en el botón **remove** en cada línea para eliminar los certificados uno a uno

Cuando se instala una nueva versión de OXO Connect Evolution, el almacén de certificados preinstalado se restablece y se carga con los de la nueva versión. Si se eliminaron algunos certificados, pero están todavía disponibles para la nueva versión, se instalan de nuevo.

Los certificados se muestran en páginas de diez. Utilice los botones de flecha en la parte superior derecha de la lista para navegar por las páginas. Pulse la tecla “Ctrl” mientras pulsa en el botón de flecha para saltar a la sexta página después de la página actual.

6.9.2. Autoridad de certificación del terminal ALE

Los certificados preinstalados incluyen la autoridad de certificación del terminal ALE, lo que permite autenticar los terminales ALE.

Dependiendo de la generación del terminal ALE, la longitud de la clave de la autoridad de certificación del terminal puede ser 1024, 2048 o 4096.

En la tabla siguiente se detallan las compatibilidades entre la longitud de la clave de la autoridad de certificación del terminal y la versión de OXO Connect Evolution.

Versión de OXO Connect Evolution	Certificado del terminal con longitud de clave de 1024/2048 bits	Certificado del terminal con longitud de clave de 4096 bits
R4.0 MD	Compatible	No soportado
R5.2	Compatible	Compatible*
R6.0 MD1	Compatible	No soportado
R6.1 o posterior	Compatible	Compatible

* OXO Connect Evolution debe actualizarse con la versión binaria compatible con la autoridad de certificación del terminal con 4096 bits.

6.9.3. Autoridades de confianza adicionales

Después de una instalación de OXO Connect Evolution desde cero, el almacén de certificados adicionales está vacío.

Puede instalar un solo certificado en formato PEM o todos los certificados contenidos en un archivo PKCS#12 protegido mediante una contraseña. Use el panel **Install new certificates** en la pestaña **Additional authorities** para instalar certificados.

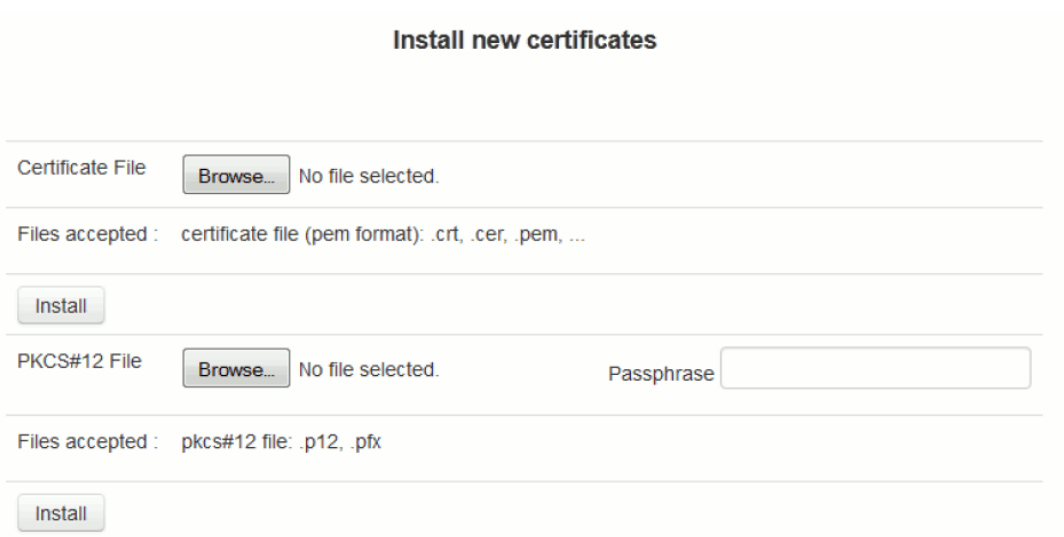


Figura 6-7 Instalación de nuevos certificados

Capítulo 6 *Gestión de certificados*

Cuando se rellena el almacén de certificados adicionales, la lista de certificados adicionales se muestra en la pestaña **Additional authorities**.

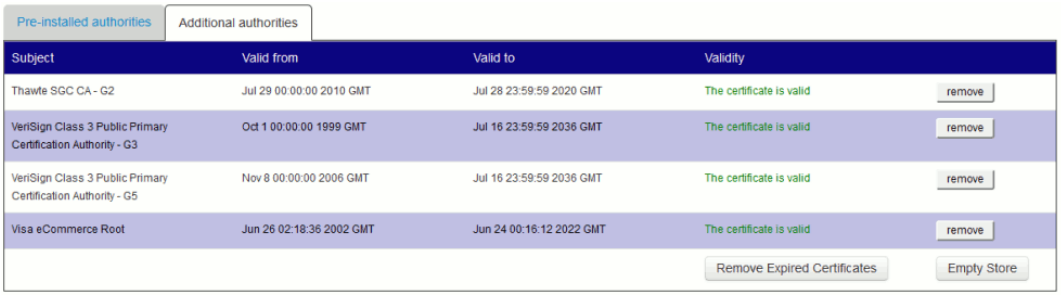


Figura 6-8 Ejemplo de lista de certificados adicionales

Por cada certificado, se muestra la información siguiente: nombre común, fechas de validez y estado de validez.

Para eliminar certificados del almacén de confianza:

- Haga clic en el botón **Empty store**, ubicado en la parte inferior de la ventana, para eliminar todos los certificados
- Haga clic en el botón **Remove Expired Certificates**, ubicado en la parte inferior de la ventana, para eliminar todos los certificados caducados
- Haga clic en el botón **remove** en cada línea para eliminar los certificados uno a uno

Cuando se instala una nueva versión de OXO Connect Evolution mediante OMC o LoLa con copia de seguridad/restauración, el almacén de certificados adicionales se mantiene en la nueva versión de OXO Connect Evolution.

Para reemplazar un certificado existente en un grupo adicional con un nuevo certificado:

1. Elimine el certificado existente
2. Instale la nueva autoridad de certificado

6.10. Implementación del certificado del servidor en los clientes

El certificado para instalar en el almacén de confianza del cliente es:

- Cuando se usa el certificado dinámico: certificado CA local: para exportar el certificado CA local, consulte Exportar el certificado CA local *(en la página 68)*

> **Nota:**
> También es posible instalar el certificado dinámico en lugar del certificado CA local, en la ventana emergente de seguridad en la primera conexión (cuando esté disponible). El certificado dinámico debe volver a instalarse en los clientes cada vez que se regenera.

- Cuando se utiliza un certificado firmado por una CA (**certificado personalizado**): el propio certificado CA.

> **Nota:**
> Cuando se instala un nuevo certificado firmado por la misma CA que el certificado actual en OXO Connect Evolution, no es necesario realizar ningún cambio en los clientes: el nuevo certificado se acepta.

El certificado de CA o el del servidor debe instalarse en:

- 4135 IP Conference Phone: consulte Implementación del certificado del servidor en 4135 IP Conference Phone *(en la página 69)*
- 8135s IP Conference Phone: consulte Implementación del certificado del servidor en 8135s IP Conference Phone *(en la página 70)*
- Almacén de confianza de Windows: consulte Implantar el certificado del servidor en Windows y navegadores web *(en la página 69)*
- Almacén de confianza del navegador web, cuando el almacén de confianza de Windows no es utilizado por el navegador: consulte Implantar el certificado del servidor en Windows y navegadores web *(en la página 69)*

6.10.1. Exportar el certificado CA local

Desde una LAN de confianza, abra un navegador web:

1. Vaya a la URL http://<nombre o dirección IP de OXO Connect Evolution> o https://<nombre o dirección IP de OXO Connect Evolution><:puerto>.
2. Haga clic en el icono **Certificate**
3. Haga clic en el enlace CA-xxxxxxxxxx.crt.
4. Guarde el archivo.

> **Nota:**
> Si la red de los clientes se considera segura, y con algunos navegadores, es posible instalar el archivo directamente haciendo clic en **Open** en vez de en **Save**, que dirige a la ventana de gestión de certificados.

6.10.2. Exportar el certificado del servidor

Realice una de las siguientes acciones:

- Desde OMC (vista Expert):
  1. Seleccione:**Importar/exportar > Exportar certificado de servidor**
  2. Haga clic en el botón Browse.
  3. Seleccione la ruta apropiada para guardar el certificado del servidor.

     Para facilitar la configuración siguiente, descargue este archivo en una llave USB.
  4. Haga clic en el botón **OK**.
- Desde una LAN de confianza, abra un navegador web:
  1. Vaya a la URL http://<nombre o dirección IP de OXO Connect Evolution> o https://<nombre o dirección IP de OXO Connect Evolution><:puerto>.
  2. Haga clic en el icono **Certificate**
  3. Haga clic en el enlace xxxxxxxxxx.crt.
  4. Guarde el archivo.

> **Nota:**
> Si la red de los clientes se considera segura, y con algunos navegadores, es posible instalar el archivo directamente haciendo clic en **Open** en vez de en **Save**, que dirige a la ventana de gestión de certificados.

6.10.3. Implantar el certificado del servidor en Windows y navegadores web

A continuación se incluye información sobre la instalación de certificados en los almacenes de confianza de Windows y el navegador web. Internet Explorer y OMC utilizan el almacén de confianza de Windows. Otros navegadores web, como Firefox, tienen su propio almacén de confianza separado.

En función de la versión de Windows, el aviso de seguridad del certificado de la página de seguridad puede sugerir o no instalarlo en el almacén de confianza.

Sin embargo, siempre es posible instalar el certificado en el almacén de confianza antes de la primera conexión. Para hacerlo, el certificado debe recuperarse en una red segura y de confianza.

Consulte Gestionar un certificado no de confianza *(en la página 70)* para obtener recomendaciones sobre la mejor forma de instalar los certificados.

En la ventana de instalación de certificados es posible elegir el almacén donde poner el certificado.

En función de la versión de Windows utilizada, el almacén de confianza predeterminado usado para el certificado puede variar.

> **Importante:**
> En cualquier caso, el certificado debe instalarse en el almacén **trusted root certification authorities store**.

6.10.4. Implementación del certificado del servidor en 4135 IP Conference Phone

Instale el certificado del servidor en 4135 IP Conference Phone a través de su página web de configuración, con el botón **root certificate**.

6.10.5. Implementación del certificado del servidor en 8135s IP Conference Phone

Instale el certificado del servidor en 8135s IP Conference Phone a través de su página web de configuración, con el botón **root certificate**.

6.10.6. Gestionar un certificado no de confianza

Si el certificado no es de confianza, el usuario de OMC puede elegir entre 3 posibilidades:

- Cerrar la conexión, considerando que no es segura
- Continuar con la conexión aceptando provisionalmente el certificado
- Instalar el certificado recibido en el almacén de confianza y continuar con la conexión

Cuando el certificado no es de confianza y no se trata del certificado dinámico, la conexión no debe aceptarse: la CA debe instalarse en el almacén de confianza de Windows.

Cuando el certificado no es de confianza y se trata del certificado dinámico, el usuario puede comprobar el contenido del certificado (nombre común, emisor, fechas de validez) para reducir el riesgo de suplantación de identidad.

Para evitar aceptar el certificado equivocado, se recomienda instalarlo antes de la primera conexión.

Cuando el certificado no es de confianza, se muestra una ventana emergente de advertencia (su aspecto depende de la versión de Windows).

El mensaje indica qué problema de seguridad se ha detectado.

Si la fecha o el nombre no son válidos, probablemente no sea seguro aceptar el certificado y la conexión no debería utilizarse. En este caso, debe generarse e instalarse un nuevo certificado (dinámico o personalizado).

Si el certificado no es de confianza, es posible inspeccionar el contenido del certificado e instalarlo en el almacén de confianza si se considera seguro.

Capítulo 7

Control de acceso

7.1. Procedimiento de configuración

7.1.1. Control de acceso global

Se deshabilita el acceso a servicios de gestión y de aplicaciones de usuario desde la WAN de forma predeterminada; este acceso puede habilitarse mediante una opción de OMC.

De forma parecida, el acceso a servicios de aplicaciones de usuario desde redes LAN está habilitado de forma predeterminada y puede bloquearse mediante una opción de OMC.

A partir de R5.2, el acceso a los servicios de gestión a través de la interfaz Ethernet **Eth1** de OXO Connect Evolution está habilitado de manera predeterminada, y puede deshabilitarse usando una opción en OMC.

Para configurar el servicio de acceso:

1. Conecte OMC a OXO Connect Evolution, bien a través de una red LAN o desde un módem remoto.
2. En OMC (vista de experto), seleccione **Seguridad** > **Servicios de red IP**
3. Revise/modifique los siguientes atributos:

Servicios de administración	
Allow Management Services from WAN	Seleccione esta casilla para permitir el uso de servicios de gestión desde una red WAN. Desactivado de forma predeterminada.
Permitir servicios de gestión en ETH1	Seleccione esta casilla para permitir el acceso a los servicios de gestión a través de la interfaz Ethernet **Eth1** de OXO Connect Evolution. Si esta casilla está desactivada, se bloquea todo el tráfico en los puertos 80 (HTTP) y 443 (HTTPS) de la interfaz **Eth1**: solo se permite el tráfico relacionado con SIP en esta interfaz. Activado de forma predeterminada.

Servicios del usuario	
External CSTA Applications authorized	Seleccione esta casilla para permitir el acceso a aplicaciones CSTA externas. Cuando está validada, esta opción abre el puerto 2555 TCP cortafuegos y de esta forma quedan autorizadas las aplicaciones CSTA externas.
Allow User Application Services from WAN	Seleccione esta casilla para permitir el uso de servicios de aplicaciones de usuario desde una red WAN. Desactivado de forma predeterminada.
Allow User Application Services from LAN	Seleccione esta casilla para permitir el uso de servicios de aplicaciones de usuario desde una red LAN. Activado de forma predeterminada.

4. Confirme las entradas

   Tras la modificación de la opción **Permitir servicios de gestión desde WAN**, **Permitir servicios de aplicación de usuario desde WAN** o **Permitir servicios de aplicación de usuario desde LAN**, OXO Connect Evolution ejecuta un reinicio en caliente.

En la siguiente tabla se muestra el estado de los clientes según el valor de las opciones de control de acceso.

Tabla 7-1 Lista de estados de cliente

Cliente	Comport. predet. en LAN	Comport. predet. en WAN	Allow Management Services from WAN Activado	Permitir servicios de gestión en ETH1 Activado	Allow User application services from WAN Activado	Allow User application services from LAN Deshabilitado
OMC	✓	✗	✓	✓		
Herramienta basada en Web	✓	✗	✓	✓		
Herramienta de diagnóstico remoto	✓	✗	✓			
ACD Statistics Manager*	✓	✗	✓		✓	
MLAA	✓	✗	✓			
Página de inicio**	✓	✗	✓	✓	✓	
Herramientas de depuración	✓	✗	✓	✓		
Facturación (OHL)	✓	✗	✓			
Banner WSDL	✓	✗	✓			
PIMphony	✓	✗			✓	✗

Capítulo 7 Control de acceso

Cliente	Comport. predet. en LAN	Comport. predet. en WAN	Allow Management Services from WAN Activado	Permitir servicios de gestión en ETH1 Activado	Allow User application services from WAN Activado	Allow User application services from LAN Deshabilitado
Dispositivos no Alcatel-Lucent Enterprise (teléfonos SIP de otros fabricantes)	✓	✗			✗	✓
4135 IP Conference Phone 8135s IP Conference Phone	✓	✗			✗	✓

* El acceso a ACD Statistics Manager solo se bloquea desde la red WAN si tanto los servicios de gestión como los de aplicaciones de usuario están bloqueados desde la WAN. Si alguno de estos servicios está activado, se puede acceder a ACD Statistics Manager desde la red WAN.

** Se permite el acceso a la página de inicio desde la red WAN si está habilitado el acceso a servicios de gestión desde WAN o a servicios de aplicaciones de usuario desde WAN. En la página de inicio, no se puede acceder a la información de ID ni de MIB desde la WAN si se han desactivado los servicios de gestión desde WAN. El acceso la página de inicio solo se bloquea desde la red WAN si tanto los servicios de gestión como los de aplicaciones de usuario están bloqueados desde la WAN.

Tabla 7-2 Lista de direcciones URL de servicio de gestión

Cliente	URL	Accesibilidad en LAN	Accesibilidad en WAN
OMC/PIMphony	/services/xmlsrv/services/XmlAdmin	✓	✓
OMC	/services/mgtsrv	✓	✓
OMC	/services/swdl	✓	✓
ACD	/services/acd_config	✓	✓
MLAA	/services/file_server/mlaa	✓	✓
Herramienta basada en Web	/services/webapp	✓	✓
Herramientas de depuración	/services/debug/traces	✓	✓
Herramientas de depuración	/services/debug	✓	✓
Herramientas de depuración	/services/debug/file_server/debug	✓	✓
MIBS	/mibs.zip	✓	✓
Página principal	/	✓	✓

Capítulo 7 Control de acceso

Cliente	URL	Accesibilidad en LAN	Accesibilidad en WAN
Facturación	/services/taxation	✓	✓
Banner WSDL	/services/free	✓	✓
Banner WSDL	/services/file_server/free	✓	✓

Tabla 7-3 Lista de direcciones URL de servicio de aplicaciones de usuario

Cliente	URL	Accesibilidad en LAN	Accesibilidad en WAN
PIMphony	/services/xlmsrv/services/XmlSuper vision	✓	✓
PIMphony	/services/xlmsrv/services/Xmlphone	✓	✓
OMC/PIMphony	/services/xmlsrv/services/XmlOxo *	✓	✓
PIMphony	/services/xmlsrv/XmlApp	✓	✓
PIMphony	/services/xmlsrv/XmlMessaging	✓	✓
ACD	/services/file_server/acd	✓	✓
ACD	/services/acd_stat**	✓	✓

* La URL `/services/xmlsrv/services/XmlOxo` solo se bloquea desde la red WAN si tanto los servicios de gestión como los de aplicaciones de usuario están bloqueados desde la WAN.

Estas son las afectaciones cuando se bloquea este URL:

- Se bloquea la ejecución/inicio de sesión de la propia aplicación PIMphony.
- No es posible el acceso/modificación de ajustes de usuario ni la adición/eliminación de supervisión de sitios desde la supervisión de PIMphony.

** La URL `/services/acd_stat` lo utiliza ACD Statistics Manager. El acceso a ACD Statistics Manager solo se bloquea desde la red WAN si tanto los servicios de gestión como los de aplicaciones de usuario están bloqueados desde la WAN.

7.1.2. Control de acceso global tras reinicio/actualización

En la tabla siguiente se indica el estado de las opciones de control de acceso tras un reinicio del sistema y en casos de migración.

Tabla 7-4 Estado de opciones de control de acceso tras reinicio del sistema o migración

Tipo de reinicio/migración	Allow Management Services from WAN	Permitir servicios de gestión en ETH1	Allow User Application Services from WAN	Allow User Application Services from LAN
Reinicio en caliente	Sin cambios	Sin cambios	Sin cambios	Sin cambios
Reinicio en frío	Predeterminado	Predeterminado	Predeterminado	Predeterminado

7.1.3. Control de acceso por abonado y aplicación

La tabla siguiente ofrece a OXO Connect Evolution conectividad de acceso en función de la aplicación o terminal y su ubicación.

Tabla 7-5 Control de acceso a API

	Acceso local	Acceso remoto
PIMphony	HTTPS para WS y eventos	HTTPS para WS y eventos (*)
OMC	HTTPS para gestión	

(*) De forma predeterminada, no se autoriza el acceso a PIMphony desde la WAN. Para autorizar el acceso:

- La opción **Allow User application services from WAN** debe estar activada
- Para cada usuario: en OMC (Expert View), seleccione: **Users/Base stations List** -> **Details**-> **Features** -> seleccione **WAN API access**

7.1.4. Denegación de acceso después de varios errores de autenticación

El acceso a la mensajería vocal de OXO Connect Evolution y a la API Web Services y API privada se controla mediante la autenticación de los usuarios con su número de teléfono (nombre de usuario) y una contraseña.

La longitud de la contraseña puede ser de cuatro o seis dígitos, según la longitud configurada en OMC: **Seguridad** > **Contraseñas** >**Contraseñas de abonados**.

Esto se aplica a los accesos locales y remotos.

Cuando un usuario ha alcanzado el número máximo de intentos de autenticación fallidos consecutivos, se deniega el acceso a este usuario. Mientras se deniega el acceso local/remoto, se rechazan todos los intentos de autenticación, aunque sean correctos.

El tiempo de bloqueo depende del número de denegaciones de acceso consecutivas.

Está fijado en diez minutos después de la primera denegación y veinte minutos después de la segunda denegación. Los tiempos de bloqueo posteriores se añaden al tiempo de bloqueo anterior hasta que el valor del tiempo de bloqueo alcanza los 1280 minutos (veinticuatro horas). Cuando el tiempo máximo de bloqueo llega a los 1280 minutos, se fija a 24 horas (1440 horas), que es el tiempo máximo de bloqueo. Cuando se alcanza el tiempo máximo de bloqueo, se mantiene para otras denegaciones, pero se pone a cero después de la correcta autenticación del usuario.

Es posible desbloquear el acceso remoto de cualquiera de las siguientes formas:

- Mediante OMC: restablece la contraseña del dispositivo bloqueado
- A través de una sesión del operador, en la configuración del abonado y acceso remoto: desbloquea el servicio de acceso remoto del usuario

Nota:
Para proporcionar el menor número de indicaciones posibles a un atacante, la notificación de una autenticación fallida es siempre igual cuando se deniega el acceso (tanto si es por haber alcanzado el máximo de intentos consecutivos o por otra razón).

Capítulo 7 Control de acceso

7.1.5. Restricciones de servicio para terminales con contraseña predeterminada

Cualquier terminal creado en OXO Connect Evolution (automáticamente o con OMC) se define con una contraseña predeterminada. Esta contraseña permite conectarse al VMU y al API Web Services. Estos servicios están restringidos para los terminales con contraseña predeterminada.

Por razones de seguridad y para permitir el acceso a esos servicios, la contraseña predeterminada debe cambiarse de manera local. No se puede modificar remotamente.

- Como para cualquier terminal, es posible modificar la contraseña usando otro terminal del sistema, llamando al grupo VMU (500 por defecto) y conectándose al VM del terminal.

7.1.6. Archivos de configuración en la red

Para evitar difundir datos importantes fuera de la red corporativa, los archivos de configuración xml solo se transmiten en la LAN, nunca en la WAN.

Cualquier cambio en el sistema que modifique la configuración de los teléfonos no se transmitirá a los teléfonos si están fuera de la LAN.

Todos los terminales deben registrarse desde la LAN para obtener sus archivos de configuración.

7.1.7. ID de mensaje aleatorio para mensajes de voz

Para aumentar la seguridad de los mensajes de voz descargados del sistema de OXO Connect Evolution y PIMphony, el formato de la ID de mensaje cambia a una ID de mensaje aleatoria en la URL para descargar un mensaje de voz.

7.1.8. Cierre del puerto FTP 30021

El puerto FTP 30021 lo utiliza la aplicación OmniVista 8770 para la supervisión y el mantenimiento de OXO Connect Evolution.

Hasta OXO Connect Evolution R5.2, el puerto FTP 30021 está abierto y no puede cerrarse.

A partir de OXO Connect Evolution R6.0 , el puerto FTP 30021 puede gestionarse a través de OMC.

1. En OMC, seleccione **Varios del sistema > Parámetros globales del sistema**
2. Revise/modifique los parámetros siguientes:

Open_FTP_Port	• **True** (valor predeterminado): el puerto está abierto • **False**: el puerto está cerrado

3. Confirme su entrada

7.2. Gestión de contraseñas

7.2.1. Supervisión

El sistema comprueba periódicamente las contraseñas (contraseñas de usuario, gestión y administrador de dispositivos) y genera los resultados como nuevos eventos históricos.

Capítulo 7 Control de acceso

Para reforzar la seguridad, se incluye información adicional relacionada con la seguridad de la contraseña en el mensaje de advertencia de seguridad de OMC, en el momento de conectarse a OXO Connect Evolution. Los mensajes de advertencia de seguridad notifican el tipo de advertencia y la ruta adecuada para modificar la contraseña a través de OMC.

Es obligatorio cambiar todas las contraseñas predeterminadas en la primera conexión a OXO Connect Evolution.

Las contraseñas del sistema se pueden supervisar para comprobar su validez y su nivel de seguridad. Desde el OMC, se puede:

- Generar la lista de abonados con la contraseña predeterminada.

  El administrador del sistema puede informar a los abonados de que pueden modificar su contraseña.

- Restablecer todas las contraseñas de los abonados.

  La opción de restablecimiento global está disponible para restablecer todas las contraseñas de los abonados a la contraseña predeterminada.

- Restablecer todas las contraseñas de los abonados con contraseñas fáciles.

  Si los abonados con contraseñas fáciles están identificados, su estado se mostrará como "Detected (Detectado)". El administrador puede restablecer las contraseñas a los valores predeterminados e informar a los abonados de que pueden modificar su contraseña.

Las contraseñas fáciles se identifican si no cumplen las reglas.

7.2.1.1. Controles automáticos de contraseñas

Este período se puede configurar en la dirección de interés AutoPwdChk. El propósito del control es identificar:

- **Contraseña predeterminada**: el sistema comprueba todas las contraseñas de gestión y de administradores de dispositivos que contienen la contraseña predeterminada.
- **Contraseña Easy**: El sistema comprueba todas las contraseñas de usuario y de gestión que no cumplen con la política de contraseñas del sistema.

7.2.1.1.1. Configuración del control automático de contraseñas

En OMC, seleccione **Varios del sistema**->**Leer/Escribir memoria**->**Depurar etiquetas.**

La comprobación automática de contraseña (AutoPwdChk) se activa con el valor predeterminado 04. Este valor representa el número de semanas entre cada comprobación automática. Los valores permitidos van del **00** al **52**.

> **Nota:**
> El control automático de contraseñas se desactiva cambiando dicho valor a **00**.

Se utiliza el comando **AutoPwdChk**:

- Inmediatamente después de modificar el valor AutoPwdChk a un valor distinto de cero.
- Regularmente en cada intervalo periódico configurado en AutoPwdChk
- Tras un reinicio en caliente.

7.2.1.1.2. Resultados del control de contraseñas

Cuando el comando de control automático de contraseñas devuelve un resultado positivo, esto significa que se han encontrado una o más contraseñas predeterminadas o fáciles. El resultado se registra como una alarma urgente y se le notifica al administrador por correo electrónico.

7.2.2. Configuraciones de contraseñas

Se accede a todas las configuraciones de contraseñas desde el OMC: **Seguridad** > **Contraseñas**

7.2.2.1. Contraseña de gestión

Si, al conectarse a OXO Connect Evolution, se detecta una contraseña predeterminada de algún administrador o usuario, OMC genera un mensaje de advertencia cada vez que inicie sesión.

Una vez que ha aparecido el mensaje de advertencia “Passwords” y se ha confirmado, aparece el estado de contraseña (predeterminado o no predeterminado) en la contraseña de administradores/ abonados predeterminados. En esta ventana se puede cambiar la contraseña del administrador o del abonado predeterminado. El instalador debe cambiar todas las contraseñas obligatoriamente para poder continuar.

La opción para restablecer contraseñas ya no está disponible en OMC.

La ventana **Management Password** ofrece la posibilidad de establecer y restablecer las contraseñas del sistema.

El acceso a la configuración de las contraseñas de gestión está limitado a las operadoras, instaladores y administradores. En la siguiente Tabla 7-6 : Reglas de acceso *(en la página 78)* se resumen las opciones de establecimiento o restablecimiento.

Tabla 7-6 Reglas de acceso

Nivel de funcionamiento OMC			
	Easy	**Easy Plus**	**Experto (Expert)**
Nivel de usuario de conexión	Operadora	Administrador	Instalador/fabricante
Tipos de usuario cuyas contraseñas se pueden restablecer Indicación del estado de la contraseña y accesos al cambio de contraseña (Botón de establecimiento)	Operadora	Operadora Administrador	Operadora Administrador Descarga Instalador NMC

En función del **nivel actual** indicado, el usuario puede acceder a los cuadros de diálogo para establecer o restablecer las contraseñas. En cada caso, para evitar el uso indebido, es obligatorio utilizar la contraseña de la sesión OMC actual y, para realizar cualquier procedimiento, se requiere confirmación.

Capítulo 7 *Control de acceso*

Nota:
Las contraseñas de gestión también pueden modificarse a través del puerto de consola, siempre que la opción **Restablecer contraseñas a través del puerto de consola** no esté desactivada. Esta opción está disponible a partir de R6.1 y se configura a través de una herramienta basada en web (para más información, consulte el documento [9]).

7.2.2.2. Contraseñas de los abonados

Se invita al instalador a configurar contraseñas predeterminadas personalizadas para los abonados.

7.2.2.2.1. Contraseñas predeterminadas

El estado de la contraseña aparece como «predeterminada» o «no predeterminada» en OMC: **Varios del sistema** -> **Contraseñas** -> **Contraseña de gestión**. Esta ventana indica el estado de contraseñas para todas las funciones.

7.2.2.2.1.1. Política de contraseñas

- La longitud de las contraseñas predeterminadas personalizadas (configuradas por el usuario) se basa en la longitud establecida en “Subscribers Password Length"
- La política de contraseñas de las contraseñas predeterminadas de abonados es la misma que para las contraseñas del resto de abonados.
- Si la contraseña personalizada de un usuario es la misma que la nueva “contraseña de abonado predeterminada”, se incluye a este usuario en la lista como “Abonado con contraseña predeterminada”.

7.2.2.2.1.2. En caso de restablecimiento o migración del sistema

La tabla siguiente indica que la gestión de contraseñas predeterminadas de abonados en situaciones de restablecimiento y migración de sistemas.

Tipo de restablecimiento o migración	Contraseña predeterminada de abonados
Reinicio en caliente	Sin cambios
Reinicio en frío	Sin cambios
Cambio sin registro de datos (igual que el reinicio en frío)	Sin cambios
Cambio con registro de datos (igual que el reinicio en caliente)	Sin cambios (restaurado)
Guardar/Restablecer EPROM	Restaurado
Restauración de OMC/migración LoLa	Restaurado

Capítulo 7 Control de acceso

Nota:
Las contraseñas predeterminadas de abonados (p. ej., 151515) y las contraseñas fáciles se sustituyen con contraseñas predeterminadas de abonados generadas de nuevo. El instalador recibe una notificación con el evento del historial "Contraseñas predeterminadas encontradas en Management/SIP Phone Administrator/Default Subscriber Password". El evento del historial 48 se modifica para incluir la notificación de la contraseña predeterminada de abonado.

7.2.2.2.2. Security level

El cuadro de diálogo de la contraseña del abonado permite a los administradores examinar el nivel de seguridad de las contraseñas utilizadas por los abonados. Se puede utilizar para:

- Conseguir la lista de abonados con la contraseña predeterminada.
- Restablecer todas las contraseñas de los abonados.
- Restablecer todas las contraseñas de los abonados con contraseñas fáciles.

  Nota:
  "Easy password (contraseña fácil)" en este contexto indica que la contraseña no cumple los requisitos de la política de contraseñas.

- Leer y especificar la contraseña predeterminada del abonado, bien con una contraseña generada de manera automática, bien con una cadena de caracteres introducidos de forma manual.

  Después de una instalación de LoLa desde cero, el sistema proporciona contraseñas predeterminadas de abonados generadas aleatoriamente, que pueden modificarse, si lo desea.

En función del nivel actual indicado, el usuario puede acceder a los cuadros de diálogo **Reset all Subscribers Password**, **Subscribers with Easy password**, **Reset all Subscribers Password** y **Default Subscribers Password**.

Para leer la contraseña predeterminada, el instalador debe autenticarse con la contraseña de sesión OMC actual.

En cada caso, para evitar el uso indebido, se requiere una confirmación y se solicita la contraseña de la sesión OMC actual.

Se accede a la ventana **Contraseña de abonados** desde el OMC: **Seguridad** -> **Contraseñas** > **Contraseñas de abonados**

El acceso a la configuración de las contraseñas de los abonados está limitado a las operadoras, instaladores y administradores. En la siguiente Tabla 7-7 : Perfil y acceso del operador del OMC *(en la página 80)* se resumen las opciones de restablecimiento o visualización.

Tabla 7-7 Perfil y acceso del operador del OMC

Nivel de funcionamiento OMC			
	Fácil (Easy)	**Easy Plus**	**Experto (Expert)**
Nivel de usuario de conexión	Operadora	Administrador	Instalador/fabricante
Muestra la longitud actual de la contraseña del abonado	Sí	Sí	Sí

Muestra la longitud planificada de la contraseña	No	No	Sí
Lista de abonados con la contrase-ña predeterminada	No	Sí	Sí
Restablecer todas las contraseñas "fáciles" de los abonados	No	Sí	Sí
Restablecer todas las contraseñas de los abonados.	No	Sí	Sí
Contraseña predeterminada de abonados	No	No	Sí

El número predeterminado de dígitos para contraseñas puede modificarse de 4 a 6, con el fin de aumentar la seguridad.

Atención:
La modificación de la longitud de la contraseña con el botón **Longitud contraseña planificada** requiere una reinicialización del sistema.

Si se detectan abonados teniendo "Default Passwords (Contraseñas predeterminadas)", el botón Detalles se vuelve disponible. Haga clic en **Detalles** para mostrar la lista de abonados y sus teléfonos.

7.2.2.3. Contraseña del administrador de dispositivos

Las contraseñas del administrador de dispositivos se encuentran disponibles en **Seguridad** > **Contraseñas** > **Contraseñas del administrador de dispositivos**.

Por defecto, el usuario no puede leer las contraseñas del administrador de dispositivos. El OMC proporciona las funciones para **leer**, **establecer** y **restablecer** contraseñas. El estado de las contraseñas (predeterminado/no predeterminado) se muestra para todos los teléfonos SIP, NOE IP y 8378 DECT IP-xBS.

El tipo de teléfono para el cual está disponible la configuración de la contraseña de administrador depende de la versión del sistema al que está conectado el OMC. Las reglas para modificar las contraseñas son las mismas que en las versiones anteriores.

Nota:
La configuración de la contraseña del administrador de dispositivos no está disponible en el modo desconectado.

Nota:
Para obtener más información sobre la **contraseña de administrador IP de NOE**, consulte Contraseña del administrador NOE IP *(en la página 82)*.

Capítulo 7 Control de acceso

7.2.2.3.1. Para leer la contraseña del administrador de dispositivos

1. Haga clic en **Read (Leer)**.
2. Escriba la contraseña de la sesión OMC actual y haga clic en **OK**.

> **Nota:**
> El botón **Leer** sólo se activa si la contraseña muestra el estado **No predeterminado**.

La contraseña del administrador de dispositivos se muestra en el campo del estado

7.2.2.3.2. Para establecer la contraseña del administrador de dispositivos

1. Para visualizar el cuadro de diálogo **Set Password (Establecer contraseña)**, haga clic en **Set (Establecer)**
2. Escriba la contraseña de la sesión OMC actual.
3. Introduzca la contraseña nueva del dispositivo.
4. Confirme la nueva contraseña del dispositivo y haga clic en **Aceptar**.

7.2.2.4. Contraseña del administrador NOE IP

Hasta OXO Connect Evolution R3.1, la **contraseña de administrador IP de NOE** se utiliza como contraseña de autenticación MMI y contraseña SSH para el acceso remoto.

A partir de OXO Connect Evolution R3.2:

1. En los terminales 8008/8008G DeskPhones, 8018 DeskPhone, 80x8s Premium DeskPhone, ALE-20/20h/30/30h Essential DeskPhone y ALE-300/400/500 Enterprise DeskPhone, la **contraseña de administrador IP de NOE** solo se utiliza para la autenticación MMI. En Contraseña SSH para acceso remoto a terminales NOE-IP *(en la página 83)*, la contraseña SSH se utiliza tanto para la autenticación SSH como MMI.
2. En 8088 Smart DeskPhone, la contraseña SSH se utiliza tanto para la autenticación SSH como MMI.

Por defecto, la autenticación MMI está habilitada con la **contraseña de administrador IP de NOE** generada aleatoriamente por OXO Connect Evolution. Para deshabilitar la autenticación MMI, la **contraseña de administrador IP de NOE** debe establecerse en un valor vacío de OMC, excepto si el **cifrado DTLS** está habilitado en OXO Connect Evolution. Si es el caso, se muestra un mensaje de advertencia que indica que la **contraseña de administrador IP de NOE** no puede estar vacía cuando el **cifrado DTLS** está habilitado.

La tabla siguiente indica la gestión de la **contraseña de administrador IP de NOE** en situaciones de restablecimiento y migración de sistemas.

Tabla 7-8 Contraseña de administrador IP de NOE en caso de restablecimiento o migración de sistemas

Tipo de restablecimiento o migración	Contraseña del administrador NOE IP
Migración de R3.1 o inferior a R3.2 o superior	Nueva contraseña generada de forma aleatoria por el sistema
Migración de R3.2 a R3.2 o superior	Sin cambios

Tipo de restablecimiento o migración	Contraseña del administrador NOE IP
Reinicio en caliente	Sin cambios
Reinicio en frío	Nueva contraseña generada de forma aleatoria por el sistema
Restablecimiento de CDB/SD CARD desde R3.1 o inferior hasta R3.2 o superior	Nueva contraseña generada de forma aleatoria por el sistema

Para modificar la **contraseña del administrador IP de NOE**:

1. En OMC, seleccione **Seguridad > Contraseñas > Contraseñas de administrador del dispositivo**
2. Haga clic en **Generar**
3. Escriba la contraseña de la sesión OMC actual.
4. Introduzca la contraseña nueva:
   - La contraseña debe contener entre 6 y 12 caracteres
   - Solo se admiten caracteres alfanuméricos
   - Los caracteres especiales no están permitidos
   - Deje un valor vacío para deshabilitar la autenticación MMI
5. Confirme la nueva contraseña del dispositivo y haga clic en **Aceptar**.

La nueva contraseña se tiene en cuenta de inmediato por todos los terminales IP NOE conectados a OXO Connect Evolution.

7.2.2.5. Contraseña SSH para acceso remoto a terminales NOE-IP

Hasta R3.1, la **contraseña de administrador IP de NOE** se utiliza como contraseña SSH para todos los terminales IP de NOE.

A partir de la versión R3.2, se genera una contraseña de sesión SSH aleatoria y se muestra para cada terminal NOE-IP cuando se activa la sesión SSH/Telnet desde la Web-Based Tool (**VoIP > VoIP Telnet Control**).

La contraseña SSH es específica para cada terminal NOE-IP y es válida solo para la sesión SSH abierta a través de la Web-Based Tool.

7.2.2.6. Contraseña de sustitución remota

El **código de control de acceso** para la sustitución remota está disponible en **Seguridad** > **Contraseñas** > **Contraseña de sustitución remota** .

El **Código de control de acceso** consta de un valor de seis dígitos generado al azar por el sistema después de la instalación de OXO Connect Evolution. Esto es igual para todos los usuarios y se aplica tanto a la sustitución remota como a la acceso remoto a la mensajería vocal.

En OMC, el botón **Read** permite ver este código.

Modifique o elimine este código dejando el campo en blanco (lo cual desactiva la función) o introduciendo un valor que tenga entre 1 y 16 dígitos.

Capítulo

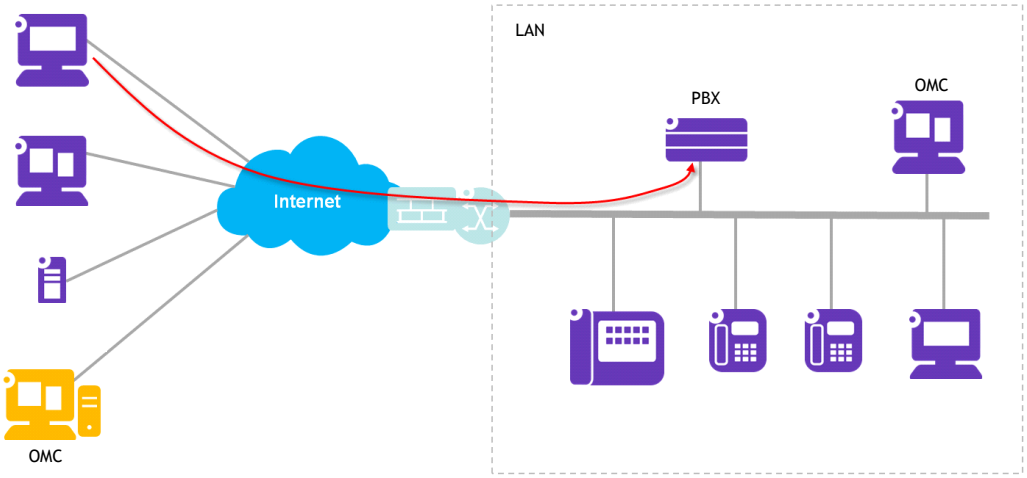
8

Configuración de la red para acceso remoto

8.1. Seguridad del acceso a Internet

Los equipos conectados a una red de área local (LAN) suelen acceder a Internet a través de un enrutador de acceso o de un dispositivo de acceso a Internet. En la actualidad, este dispositivo incluye sistemáticamente funciones de cortafuegos para proteger de amenazas externas a la LAN.

OXO Connect Evolution no está conectado directamente a Internet, sino a la LAN. El acceso remoto a OXO Connect Evolution desde Internet suele realizarse a través del dispositivo de acceso a Internet que tiene funciones de cortafuegos en la frontera de la LAN. El acceso remoto pueden requerirlo tanto aplicaciones del usuario final PIMphony como aplicaciones de gestión (OMC y Web-Based Tool).



Por lo tanto, es muy importante aplicar las medidas de seguridad adecuadas en la configuración del dispositivo de acceso a Internet/cortafuegos para garantizar un acceso remoto protegido al servidor de OXO Connect Evolution.

El acceso remoto se debe activar únicamente si es necesario. Cuando se necesite acceso remoto, emplee con detenimiento todas las recomendaciones incluidas en las siguientes secciones relativas a su versión del producto.

8.2. Acceso remoto a OXO Connect Evolution

Los servicios remotos a través de Internet son posibles, pero requieren la observación de los principios de seguridad que se incluyen a continuación. Recuerde que OXO Connect Evolution está conectado a la LAN y no directamente a Internet.

El sistema distingue las conexiones que se originan en Internet y en la LAN a partir de las direcciones de los puertos en el propio OXO Connect Evolution:

- Los puertos 443 y 10443 están dedicados a conexiones procedentes de la LAN.
- El puerto 11443 está dedicado al certificado estático de HAP
- El puerto 50443 está dedicado a conexiones procedentes de Internet y utiliza políticas de control de acceso adaptadas.

Capítulo 8 *Configuración de la red para acceso remoto*

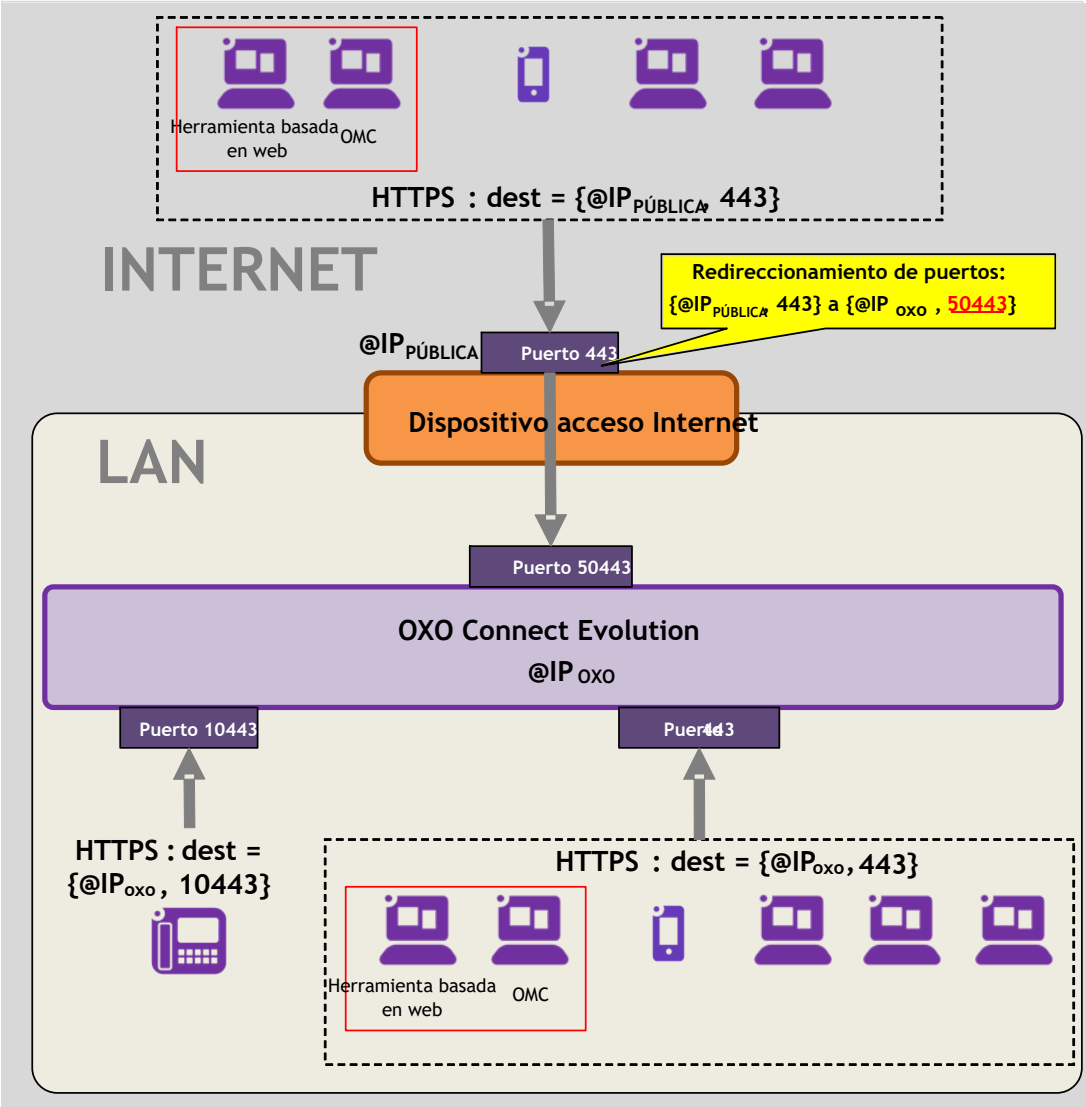


Figura 8-1 OXO Connect Evolution

Cualquier acceso remoto desde Internet se recibe en la interfaz pública del dispositivo de acceso a Internet, que reenvía el tráfico recibido al sistema de OXO Connect Evolution de la LAN.

Las aplicaciones que se conectan a OXO Connect Evolution desde Internet deben utilizar el protocolo HTTPS. El puerto de destino predeterminado utilizado por las aplicaciones es el puerto HTTPS estándar 443. En algunos casos, puede utilizarse otro puerto, consulte Acceso remoto a OXO Connect Evolution cuando el puerto público 443 está ocupado *(en la página 86)*.

El redireccionamiento de puertos en el dispositivo de acceso a Internet debe estar configurado para redireccionar el tráfico entrante recibido en el puerto público 443 al puerto 50443 de OXO Connect Evolution:

- Reenviar {@IPPUBLIC, puerto 443} a {@IPOXO, puerto **50443**}

Capítulo 8 *Configuración de la red para acceso remoto*

Atención:

- Para el acceso remoto desde Internet con reenvío a OXO Connect Evolution, el puerto de destino en OXO Connect Evolution siempre debe ser el 50443.
- No reenvíe ningún tráfico procedente de Internet a otro puerto de OXO Connect Evolution distinto del 50443, a excepción de los puertos explícitamente requeridos para la activación de servicios de enlaces IP.
- No reenvíe ningún tráfico de Internet a los puertos 443 o 10443.

Nota:
En esta topología, pueden utilizarse conexiones basadas en VPN para las aplicaciones remotas (consulte Acceso remoto a OXO Connect Evolution con VPN *(en la página 86)*).

Importante:
En caso de una conexión remota, la solución basada en VPN es la única solución posible para PIMphony IP.

8.3. Acceso remoto a OXO Connect Evolution con VPN

La solución Cloud Connect permite establecer una conexión VPN entre OXO Connect Evolution y las aplicaciones mediante una pasarela VPN alojada en el centro de servicio remoto.

Para obtener más información sobre la aplicación de esta solución, consulte:

- El manual de instalación de OXO Connect Evolution
- 8AL91215ENAA: Cloud Connect VPN Server Reference Design

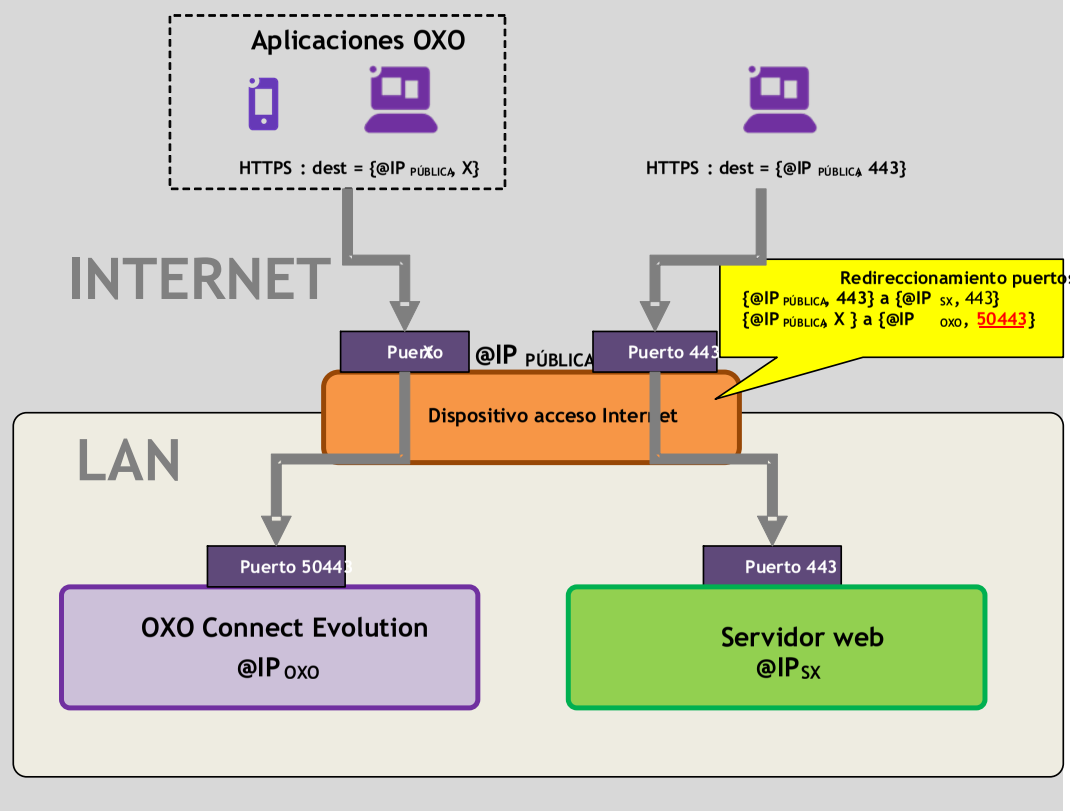
8.4. Acceso remoto a OXO Connect Evolution cuando el puerto público 443 está ocupado

Partimos de la base de que el dispositivo de acceso a Internet tiene asignada una sola dirección IP pública.

Si hay otro servidor HTTPS (por ejemplo, un servidor web) conectado a la LAN, además del sistema de OXO Connect Evolution, se deben utilizar puertos diferentes del dispositivo de acceso a Internet para dirigir a cada servidor desde Internet. Un puerto puede ser el puerto HTTPS estándar 443. El otro puerto puede ser cualquiera de los puertos del dispositivo de acceso a Internet que no se estén utilizando.

Capítulo 8 *Configuración de la red para acceso remoto*

Recuerde que el puerto de destino utilizado por las aplicaciones que se conectan a OXO Connect Evolution desde Internet **no** es un puerto de OXO Connect Evolution, sino un puerto de la interfaz pública del dispositivo de acceso a Internet. Cualquier tráfico recibido en este puerto público, el dispositivo de acceso a Internet lo reenviará al puerto 50443 local del sistema de OXO Connect Evolution en la LAN.



Configuración genérica:

- Para conectarse a OXO Connect Evolution desde Internet, utilice la dirección de destino {@IPPUBLIC, puerto X}.
- Para conectarse al servidor web desde Internet, utilice la dirección de destino {@IPPUBLIC, puerto 443}.

El redireccionamiento de puertos debe estar configurado igualmente en el dispositivo de acceso a Internet:

- Reenviar {@IPPUBLIC, puerto X} a {@IPOXO, puerto 50443}
- Reenviar {@IPPUBLIC, puerto 443} a {@IPSX, puerto 443}

Capítulo 8 *Configuración de la red para acceso remoto*

Atención:

- Para el acceso remoto desde Internet con reenvío a OXO Connect Evolution, el puerto de destino en OXO Connect Evolution siempre debe ser el 50443.
- No reenvíe ningún tráfico procedente de Internet a otro puerto de OXO Connect Evolution distinto del 50443, a excepción de los puertos explícitamente requeridos para la activación de servicios de enlaces IP.
- No reenvíe ningún tráfico de Internet a los puertos 443 o 10443.

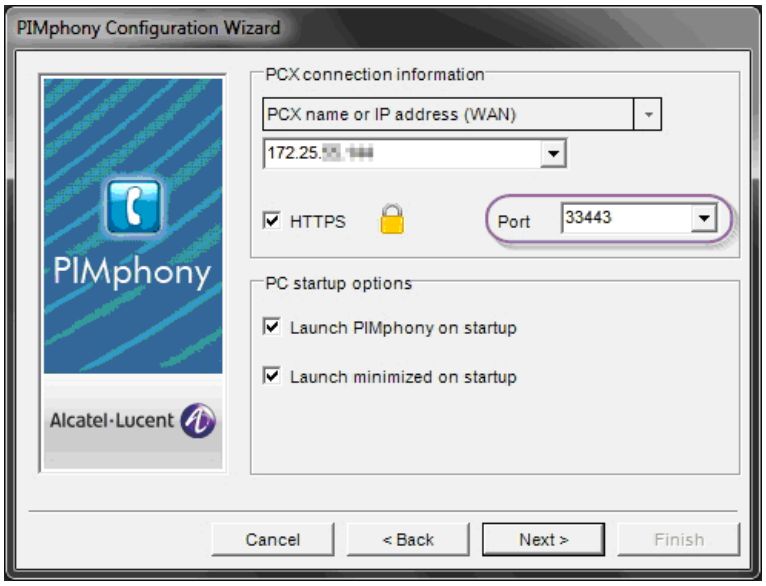
8.4.1. Configuración de puerto de conexión para aplicaciones de usuario final

Si se utiliza un puerto público de destino distinto del HTTPS estándar 443 en el dispositivo de acceso a Internet, es preciso configurarlo como puerto de destino nuevo para cada aplicación de usuario final.

Tenga presente que puede utilizar cualquiera de los puertos del dispositivo de acceso a Internet que no se estén utilizando. Debe emplearse el mismo puerto para todas las aplicaciones.

8.4.1.1. PIMphony

En cuanto a PIMphony (PIMphony asociado a un terminal físico de OXO Connect Evolution), el puerto de destino utilizado para la conexión remota debe definirse en el asistente de configuración:



8.4.2. Configuración de puerto de conexión para aplicaciones de gestión

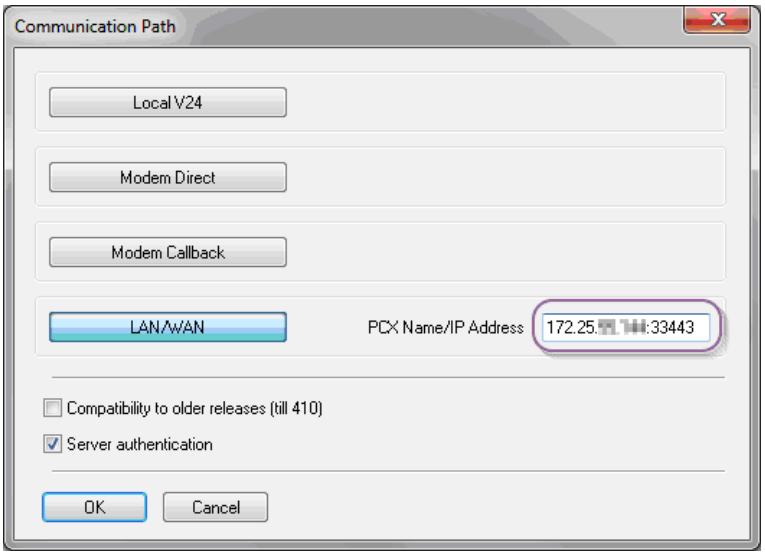
Si se utiliza un puerto público de destino distinto del HTTPS estándar 443 en el dispositivo de acceso a Internet, es preciso configurarlo como puerto de destino nuevo para cada aplicación de gestión.

Tenga presente que puede utilizar cualquiera de los puertos del dispositivo de acceso a Internet que no se estén utilizando. Debe emplearse el mismo puerto para todas las aplicaciones.

8.4.2.1. OMC

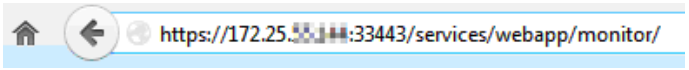
El puerto de destino predeterminado es 443.

El puerto de destino se puede definir con el nombre de host/dirección IP del sistema en la ventana de conexión que se muestra:



8.4.2.2. Web-Based Tool

La Web-Based Tool es una aplicación web: el puerto de destino se puede definir en el navegador web.



Capítulo 9

SMTP seguro

9.1. Introducción

El OXO Connect Evolution puede enviar correos electrónicos tanto a través de MTA básicos sin STARTTLS como de MTA seguros con STARTTLS, cuando lo solicite el servidor.

Solo se admite STARTTLS. La otra solución (obsoleta), que consiste en abrir una sesión de sendmail a través de TLS, no está implementada.

Cuando se establece la conexión segura, la autenticación se produce con normalidad. Los métodos de autenticación permitidos son: LOGIN, PLAIN, DIGEST-MD5, CRAM-MD5 y NTLM.

El certificado de CA que firmó el certificado utilizado para SMTP debe cargarse en un almacén de confianza de OXO Connect Evolution.

El certificado utilizado para SMTP debe contener el nombre de dominio totalmente cualificado del servidor de correo (por ejemplo, el FQDN del servidor de intercambio).

9.2. Procedimiento de configuración

La configuración de MTA consta de:

- La configuración de la dirección del servidor y, si es necesario, el número de puerto en OMC: **Central Services Global Info** > **Email Notification** > **Admin Email address**

  Por defecto, el puerto utilizado por sendmail para conectarse al MTA es el puerto 25 (puerto legado). Cuando deba utilizarse otro puerto, por ejemplo, el puerto de envío (587), debe añadirse el número de puerto a la dirección del **E-mail Notification Server** configurada en OMC, por ejemplo, **smtp.googlemail.com:587**.

- La configuración de una cuenta válida (nombre de inicio de sesión y contraseña) para el MTA en OMC: **Central Services Global Info** > **Email Notification** > **SMTP Authentication**

  Esta cuenta es el origen de los correos electrónicos enviados por el sistema.

- Para cada terminal configurado para activar notificaciones:
  - La configuración de la dirección de correo electrónico de origen en OMC: **Subscribers** > **Cent. Serv.** > **User** > **Email address**

    La dirección de correo electrónico de origen configurada debe ser la dirección de correo electrónico de la cuenta utilizada para iniciar sesión.
  - La configuración del destinatario de las notificaciones en OMC: **Subscribers** > **Cent. Serv.** > **Email Notification** > **Email Notification Address**

Para obtener más información sobre configuración, consulte la sección **Notificación por correo electrónico** del documento [3].

Capítulo

10

Aprovisionamiento automático

Si los terminales tienen que inicializarse de forma dinámica, debe activarse el aprovisionamiento automático en la configuración de OXO Connect Evolution.

Para facilitar la instalación del sistema, la mayor parte de los teléfonos IP Alcatel-Lucent Enterprise se detectan de forma automática y se registran en el sistema al conectarse. Así, estos teléfonos IP se encuentran plenamente operativos sin que el administrador del sistema tenga que realizar ninguna acción.

Esto es aplicable a:

- Teléfonos Alcatel-Lucent Enterprise IP
- Teléfonos Alcatel-Lucent Enterprise SIP

La función de aprovisionamiento automático solo es aplicable a teléfonos IP que se registran de forma automática en el sistema de OXO Connect Evolution.

En la siguiente tabla se muestra una lista de teléfonos IP y se indica su compatibilidad con el aprovisionamiento automático en el sistema de OXO Connect Evolution.

Tabla 10-1 Lista de teléfonos IP y compatibilidad con el aprovisionamiento automático

Teléfonos IP/aplicaciones	Compatibilidad con el aprovisionamiento automático
80x8 Premium DeskPhone	Compatible
80x8s Premium DeskPhone	Compatible
ALE-300/400/500 Enterprise DeskPhone	Compatible
ALE-20/20h/30/30h Essential DeskPhone	Compatible
ALE-2 DeskPhone	Compatible
ALE-3 DeskPhone	Compatible
4135 IP Conference Phone	Compatible
8135s IP Conference Phone	Compatible
8008/8008G CE DeskPhones	Compatible
8088 Smart DeskPhone	Compatible
Teléfono 82x2 DECT	No soportado
8214/8234/8244/8254 DECT	No soportado
MIPT	Compatible
8018 DeskPhone/80x8s Premium DeskPhone, ALE-300 Enterprise DeskPhoneALE-400 Enterprise DeskPhoneALE-500 Enterprise DeskPhone, ALE-20/20h/30/30h Essential DeskPhone con compatibilidad con VPN remota	Compatible

Capítulo 10 *Aprovisionamiento automático*

Teléfonos IP/aplicaciones	Compatibilidad con el aprovisionamiento automático
IP Desktop Softphone	Compatible
PIMphony IP	No soportado

Nota:
Debe crearse un terminal en OMC de forma manual

Si el aprovisionamiento automático está activado, pueden conectarse nuevos teléfonos IP, que se registran de forma automática en el sistema.

Si el aprovisionamiento automático está desactivado, se rechazan los nuevos teléfonos IP que se conectan al sistema.

El aprovisionamiento automático se activa de forma temporal durante un período predefinido (8 horas). El aprovisionamiento automático se desactiva al finalizar dicho período.

10.1. Configuración del aprovisionamiento automático mediante OMC

1. En OMC, vaya a **Subscribers/Basestations List** > **Auto Provision**

   Se abre la ventana de aprovisionamiento automático
2. Haga clic en **Activate temporarily**

   El aprovisionamiento automático se activa de forma temporal durante un período predefinido (8 horas)
3. Cierre y vuelva a abrir la pantalla para ver el cambio de estado

   El estado de la configuración del aprovisionamiento automático se indica en la parte inferior de la pantalla de la lista **Subscribers/Base stations**: *Automatic provisioning temporarily activated* o *Automatic provisioning deactivated*

10.2. Configuración del aprovisionamiento automático mediante DHM

La función de aprovisionamiento automático puede activarse o desactivarse desde el teléfono DHM.

1. En DHM, abra una sesión de administrador: **Menu** > **System** > **Admin**
2. Introducir la contraseña de administrador
3. En la ventana **System Prog**, seleccione la opción **Auto.Prov.**

   Se muestra el estado actual de la función de aprovisionamiento automático

Capítulo 10 *Aprovisionamiento automático*

4. Seleccione un valor:
   - **ON**: pulse el botón **ON** para activar el aprovisionamiento automático

     Se muestra el siguiente mensaje: *Auto Provisioning activated*
   - **OFF**: pulse el botón **OFF** para desactivar el aprovisionamiento automático

     Se muestra el siguiente mensaje: *Auto Provisioning deactivated*
5. Haga clic en el icono **Back**, situado en la esquina derecha, para volver al menú anterior