INDAP | Cultivando tradiciones, cosechando futuro.
Ministerio de Agricultura

APRUEBA CONTRATO PARA LA CONTRATACIÓN DE LOS SERVICIOS DE PLATAFORMA DE SEGURIDAD Y CONTROL PERIMETRAL DE INDAP CON LA EMPRESA NETICS SPA, Y AUTORIZA MODALIDAD DE TRATO DIRECTO QUE INDICA

SANTIAGO, 13/ 06/ 2025

RESOLUCIÓN AFECTA Nº: 0070-000015/2025

VISTOS:

La Ley N° 18.910 Orgánica del Instituto de Desarrollo Agropecuario, y sus modificaciones; la Ley N° 19.886 sobre contratos administrativos de suministro y prestación de servicios; el Decreto Supremo N° 250 de 2004 del Ministerio de Hacienda, el Decreto Supremo N° 661 de 2024, del Ministerio de Hacienda, que aprueba el Reglamento de la Ley N° 19.886; la Ley N° 21.722 de presupuestos del Sector Público correspondiente al año 2025; el Decreto N° 46 de 28 de abril de 2022 del Ministerio de Agricultura, que nombra al Director Nacional del Instituto de Desarrollo Agropecuario y Decreto Exento N°64 de 03 de mayo de 2023 del Ministerio de Agricultura; la Resolución 36 de 2024, que fija normas sobre exención del trámite de toma de razón y establece controles de reemplazo cuando corresponda, ambas de la Contraloría General de la República; y,

CONSIDERANDO:

1.-Que, mediante Resolución Afecta N° 0070-000052/2024, de fecha 21 de octubre de 2024 de la Dirección Nacional de INDAP, tomada de razón el 04 de noviembre de 2024 por la Contraloría General de la República, se aprobaron las bases de licitación pública para la contratación de los servicios de telecomunicaciones de INDAP por un periodo de 60 meses, publicadas en el sistema de Mercado Público según ID 609-91-LR24.

2.- Que, mediante Resolución Exenta N° 0070-005414/2025 de fecha 12.02.2025 de la Dirección Nacional de INDAP, se adjudicó la licitación pública a la propuesta presentada por la empresa PACÍFICO CABLE SPA, por ser la propuesta más favorable técnica y económicamente a los intereses de INDAP, de acuerdo al informe de evaluación técnica y económica de fecha 4 de febrero de 2025, correspondiente al ID 609-91-LR24.

3.- Que, INDAP y la empresa adjudicada suscribieron un contrato, de fecha 18 de febrero de 2025, para la prestación de los servicios de telecomunicaciones de INDAP, con una vigencia de 60 meses a contar de la fecha de inicio de operación de los servicios, y por un monto total de UF 161.833,8 (ciento sesenta y un mil ochocientos treinta y tres coma ocho unidades de fomento), impuestos incluidos, el que fue aprobado por Resolución Afecta N° 04/2025, de 27.02.2025, que fue remitido en su oportunidad al trámite de toma de razón ante la Contraloría General de la República, sin embargo mientras se tramitaba dicho control de juridicidad, la otra empresa que participó en el proceso y quien presentó una oferta 100% superior al presupuesto estimado contemplado por este Instituto, interpuso una acción ante el Tribunal de Contratación Pública (Causa Rol 66-2025), y consecuencia de ello, con fecha 03.03.2025 se ordenó la suspensión del referido proceso licitatorio hasta la dictación del respectivo fallo del mencionado tribunal lo que acaeció con fecha 03.06.2025.

4.- Que, el contrato de los servicios de telecomunicaciones que dispone actualmente INDAP, termina su vigencia el día 02.10.2025, y no prevé posibilidades de extensión, toda vez que ya fue renovado y en virtud de ello expira en la data antes mencionada, y que aun cuando existieran dichas posibilidades de extensión, en razón de la obsolescencia de sus componentes (contrato aprobado en el año 2019), aquel no daría garantías ni daría cumplimiento a los estándares normativos que deben ajustarse los organismos de la Administración del Estado, relacionados con Ciberseguridad e Infraestructura Crítica de la Información, y con Protección de Datos Personales, entre otros.

5.- Que, el referido proceso judicial se encuentra actualmente en tramitación y discusión y será objeto de conocimiento de los tribunales superiores de justicia – en virtud del recurso de apelación que prevé la ley 19.886-, ello por un curso de tiempo que este Servicio no puede ponderar con exactitud; sin embargo, dicha tramitación judicial pendiente y que contempló suspensiones sucesivas del proceso de contratación en cuestión, da cuenta evidentemente, de que este Servicio ha quedado desprovisto en la especie, de utilizar el mecanismo concursal de licitación pública para la provisión y continuidad de los servicios de telecomunicaciones –los cuales expiran el 02.10.2025, que por cierto, son esenciales para la operación de un servicio público, ya que en su ausencia en estricto [illegible]ría viable cumplir con el mandato legal otorgado a esta institución.

6.- Que, en ese sentido, aun cuando este Instituto, inicie el proce[illegible]ción de bases de licitación, no debe perderse de vista que un proceso de licitación de esta envergadura po[illegible]; asociados y por lo diferentes controles

TOMADO DE RAZÓN CON ALCANCES
Oficio: E108489/2025
POR ORDEN DE LA CONTRALORA GENERAL DE LA REPÚBLICA
Fecha: 06/06/2025
JUAN JOSE MONTERO PORTER
Subcontralor General

de juridicidad a los que debe ser sometido, requieren un plazo extenso que en ningún caso se podría cumplir para dar continuidad a servicios de esta naturaleza indispensable desde el 02.10.2025, cuestión que como ya se dijo pondría en riesgo la continuidad operativa de INDAP.

7.- Que, sin perjuicio de que las bases de licitación se encuentran supeditadas al resultado del proceso judicial actualmente en tramitación, es necesario tener presente que, de acuerdo con la experiencia institucional en causas de similar naturaleza, la resolución de dicho proceso en curso, podría demorar un período estimado de ocho meses en sede de la Iltma. Corte de Apelaciones respectiva, y hasta un año adicional en caso de que sea sometido al conocimiento de la Excma. Corte Suprema. Tal dilación, en caso de no adoptarse decisiones administrativas de continuidad, podría poner en riesgo la adecuada prestación del servicio, afectando gravemente el cumplimiento de funciones institucionales esenciales.

8.- Que, a lo anterior, se suma que servicios como los que se requieren en la licitación objetada, necesitan de un tiempo de implementación mínimo que va de los 6 a 8 meses – dependiendo del tipo de tecnologías y recursos ofertados-, razón por la cual para evaluar la continuidad operacional del servicio se debe ponderar efectuar un ajuste a las condiciones técnicas allí previstas a fin de que determinados proveedores estén en condiciones técnicas y económicas para la prestación de los servicios.

9.- Que, por su parte, adicionalmente, debe tenerse a la vista que los montos involucrados en este tipo de servicios corresponden a contratos con componentes de infraestructura y soporte que requieren amortización a mediano plazo (generalmente al menos 36 meses). En el caso del proceso licitatorio ID 609-91-LR24, la contratación proyectada era por 60 meses, lo que permitía al proveedor distribuir costos fijos de instalación, equipamiento y adecuaciones técnicas y con ello hacer más eficiente la contratación para el Instituto.

10.- Que, en ese sentido para evaluar una contratación de continuidad y aun cuando se proyecte un plazo mínimo acotado, conforme a las condiciones disponibles en el mercado, ello no sería viable por menos de 24 meses, plazo que de igual manera dice relación con el tiempo necesario que podría llevar un nuevo proceso de licitación pública.

11.- Que, como ya se indicó la contratación de los servicios de telecomunicaciones de INDAP, constituye un servicio crítico y estratégico considerando que esta Institución cuenta con 16 Direcciones Regionales, 116 Agencias de Áreas y 22 oficinas de Área, atendiendo aproximadamente a más de 270.000 usuarios, y cuenta con un presupuesto asignado de M$406.206.221 para el año 2025, por lo que en el supuesto de no disponer de dicho servicio de telecomunicaciones, INDAP se encontraría impedido de funcionar adecuadamente, e incluso podría sufrir la pérdida de información que es esencial para la Institución, por lo que resulta imperioso asegurar la continuidad operacional toda vez que aquello obedece a razones de interés público.

12.- Que, sin perjuicio de lo señalado es del caso tener presente que la referencia de interés público dice relación con aquel valor, beneficio o bien jurídico que satisface el conjunto de los derechos fundamentales, así como de los intereses individuales y colectivos de todos y cada uno de los integrantes de la sociedad civil. En este sentido, la Constitución política de 1980, al referirse al fin del Estado, en el inciso 4° de su artículo 1°, señala: “El Estado está al servicio de la persona humana y su finalidad es promover el bien común, para lo cual debe contribuir a crear las condiciones sociales que permitan a todos y a cada uno de los integrantes de la comunidad nacional su mayor realización...”

13.- Que, en ese sentido el interés público debe ser concebido como un conjunto de necesidades y aspiraciones de la sociedad que el Estado debe satisfacer y promover, priorizando el bienestar colectivo sobre intereses particulares, cuestión que se fundamenta en principios constitucionales y normativos que orientan la función pública hacia la consecución del bien común, por lo que constituye uno de los fundamentos esenciales del actuar de los Organismos de la Administración del Estado y se materializa cuando las actuaciones públicas buscan garantizar derechos fundamentales, proteger bienes comunes y promover el bienestar general, debiendo dichas actuaciones relacionarse directamente con los objetivos esenciales del Estado.

14.- Que, con el objeto de no afectar dicho interés público y la operatividad de INDAP, se requiere utilizar en este caso excepcional e imprevisto (por la tramitación judicial inesperada que afectó al proceso destinado a la contratación por vía concursal de los servicios) efectuar una contratación directa para, por una parte dar cobertura y continuidad a los servicios de comunicaciones institucionales y por otra, para dar cobertura a las plataformas de seguridad y control perimetral de INDAP incluyendo Data Center, ello mientras se levanta y tramita un nuevo proceso de licitación pública que considere en una única contratación dichos servicios y con condiciones de vigencia y técnicas asimilables a las del proceso de licitación que fuera objetada.

15.- Que, el artículo 8 bis, de la Ley 19.886, establece que :Procederá el Trato Directo o Contratación Excepcional Directa con Publicidad en los casos fundados que a continuación se señalan: c) En casos de emergencia, urgencia o imprevisto, en que se requiera satisfacer una necesidad pública de manera impostergable, siempre que se justifique que, en caso de no realizarse la contratación en un breve plazo, se generarían graves perjuicios a las personas o al funcionamiento del Estado, calificados mediante resolución fundada del jefe superior del organismo contratante, y que, para evitar dichos perjuicios, no pueda utilizarse otro procedimiento de contratación. Lo anterior, sin perjuicio de las disposiciones especiales para casos de sismos y catástrofes contenidas en la legislación pertinente. En caso que las circunstancias que justifiquen la aplicación de esta causal sean imputables a la entidad pública contratante, deberán adoptarse oportunamente las medidas tendientes para determinar las eventuales responsabilidades administrativas que correspondan. En los contratos que se suscriban justificados en esta causa, el plazo para efectuar el suministro o prestación del servicio deberá ser delimitado a los supuestos de hecho que lo fundan”.

16.- Que, por su parte el artículo 71 del Reglamento de Compras Públicas contenido en el Decreto Supremo N° 661 de 2024, establece que: “Excepcionalmente, procederá el Trato Directo o [illegible]ción Excepcional Directa con Publicidad

en los casos fundados y conforme a las normas que se establecen en la Ley de Compras y en el presente Capítulo. Las causales de Trato Directo son las que a continuación se señalan: 3. En casos de emergencia, urgencia o imprevisto, en que se requiera satisfacer una necesidad pública de manera impostergable, sin perjuicio de las disposiciones especiales para casos de sismos y catástrofes contenidas en la legislación pertinente".

17.- Que, por su parte, el artículo 74 del mencionado reglamento establece, en lo que interesa, que: "Trato directo por emergencia, urgencia e imprevisto. Para efectos de la aplicación de esta causal, se entenderá que: b) La urgencia se refiere a aquella necesidad apremiante, que solo puede ser satisfecha si se obtiene la prestación requerida en el menor tiempo posible, y cuya falta de ejecución generará perjuicios en las personas, el funcionamiento o los bienes de la Entidad. c) El imprevisto es aquella circunstancia de hecho externa y fortuita que no es posible resistir, y que impide el normal funcionamiento de la Entidad que requiere la contratación. El acto administrativo fundado de la jefatura superior del servicio que autorice la contratación mediante esta causal deberá contener: a) Los supuestos de hecho que justifican que, en caso de no realizarse esta contratación en un plazo breve, se generarían graves perjuicios a las personas o al funcionamiento del Estado. b) Los motivos de porque no puede utilizarse otro procedimiento de contratación para evitar que estos perjuicios ocurran. En los contratos que se suscriban justificados en esta causal, el plazo para efectuar el suministro o prestación del servicio deberá ser delimitado a los supuestos de hecho que lo motivan".

18.- Que, la situación imprevista, apremiante y excepcional en la que se encuentra INDAP, configuraría en la especie la causal de trato directo antes descrita, toda vez que fue provocada por un proceso judicial imprevisto, que ha impedido efectuar cualquier tipo de contratación para proveer la continuidad de las telecomunicaciones; el no llevar a cabo una contratación de esta naturaleza, implicaría un perjuicio tanto para este Servicio, para sus usuarios y para el adecuado funcionamiento de la Administración del Estado, quien no podría cumplir su mandato afectando el interés público; y en el evento de utilizar otro mecanismo de contratación, en razón como ya se dijo de los tiempos de tramitación ordinario de un proceso concursal –por los montos asociados- y los tiempos de implementación de los servicios que se requieren, no se evitaría la afectación del interés público que se pretende proteger con la utilización de esta modalidad de contratación directa.

19.- Que lo anterior, no es de menor importancia, toda vez que, en virtud del principio de continuidad del servicio público, la Administración no puede quedar desprovista de servicios esenciales para su funcionamiento operativo. La ausencia de conectividad, seguridad digital o acceso a redes institucionales afecta la gobernanza digital y pone en riesgo incluso el cumplimiento de metas y compromisos institucionales con otros organismos del Estado y con sus beneficiarios, y afectando adicionalmente servicios de conexión con otras plataformas del Estado, trámites ciudadanos y servicios de atención remota a más de 154 oficinas y agencias que INDAP tiene desplegado a lo largo del país.

20.- Que, al respecto es pertinente señalar la población usuaria de INDAP corresponden a pequeños productores agrícolas y campesinos (Ley Orgánica de INDAP) que se caracterizan por pertenecer en su mayoría al Tramo 1 de calificación socioeconómica del Registro Social de Hogares (RSH), que corresponde a los hogares calificados en el 40% de menores ingresos, lo que representa al segmento de mayor vulnerabilidad de la población nacional; además un 37% de las/os usuarias/os se declara ser parte de un pueblo originario. Cumple con su misión institucional a través de 21 programas de fomento productivo y asistencia financiera de corto y largo plazo (programa de crédito), prestando atención aproximadamente a 170 mil usuarios a nivel nacional. Uno de los programas de fomento productivo de mayor impacto corresponde al Programa de Desarrollo Local PRODESAL, el cual atiende a una población aproximada de 70 mil usuarios/as y que se despliega a nivel nacional a través de convenios con 260 municipios y la atención de 1900 extensionistas desde Arica y Parinacota a la región de Magallanes. Por otra parte, la atención crediticia del Instituto es diaria concurriendo nuestros usuarios a las diferentes oficinas institucionales a fin de solicitar financiamiento parcial para el fomento y/o desarrollo de actividades productivas, comerciales y de servicios, de carácter silvo-agropecuario y otras que se ajusten a los objetivos institucionales y que demuestren ser económica y financieramente convenientes de ejecutar, es así que a junio 2025 se colocaran M$ 58.9710.210.- para 20.855 usuarios/as del Instituto. Adicionalmente durante el año 2024 INDAP obtuvo el premio a la excelencia institucional, y dentro de las iniciativas postuladas en dicha oportunidad es pertinente relevar Mi pago INDAP, el cual consiste en un portal fundamental en la modernización y la transformación digital del Instituto, a través de esta herramienta digital las y los usuarios puedan pagar y acceder a su información crediticia de manera actualizada y durante las 24 horas de los siete días de la semana.

21.- Que, como es posible vislumbrar a través de este somero resumen de la actividad institucional, mantener operativos los servicios de comunicaciones y de plataforma de seguridad y control perimetral para el Instituto pasa a ser un aspecto vital para el cumplimiento de su obligación legal y continuidad en la provisión de los programas y servicios que debe otorgar a la ciudadanía, su mantención en esencial y crítico para permitir la operación crediticia diaria, la gestión y ejecución de los diversos programas de fomento productivo, así como el resguardo y protección de los datos personales y crediticios de nuestros usuarios.

22.-Que, como se indicó previamente para la utilización de esta modalidad excepcional, se considera el mínimo de tiempo razonable, conforme a las condiciones disponibles en el mercado, lo que no sería viable por menos de 24 meses, plazo que de igual manera dice relación con el eventual tiempo necesario para un nuevo proceso de licitación pública, el cual podría fluctuar entre 10 a 12 meses más el tiempo para la implementación de un contrato de las características como el que fue licitado.

23.-Que, en el caso de la especie, tal como se ha manifestado en los Considerando precedente, el fundamento de emergencia o urgencia para la aplicación de la causal de Trato Directo, en ningún caso dice relación con la falta de gestión oportuna de los procedimientos necesarios de INDAP para [illegible] la continuidad de las prestaciones ya aludidas, así como tampoco la falta de ejecución total o parcia[illegible] oyectos o prestaciones originalmente contemplados en un contrato previamente celebrado entre las mism[illegible] y tampoco deriva de una planificación inadecuada del Servicio, por cuanto como ya se indicó, la situación a[illegible] que se encuentra INDAP, obedece a la

tramitación imprevista de un proceso judicial que se encuentra pendiente, el que de no haber mediado, hubiese permitido a INDAP holgadamente (mes de marzo de 2025) y con varios meses de anticipación tener preparada tanto la implementación de los servicios como el inicio de su ejecución y la continuidad operativa derivada de ello a contar del 02.10.2025.

24.- Que, efectuada una invitación a los proveedores que pudiesen dar continuidad de los servicios de comunicaciones institucionales y de plataformas de seguridad y control perimetral de INDAP, en las condiciones técnicas y económicas ajustadas para una contratación de 24 meses, que está por debajo de la proyección ordinaria de 36 meses de cualquier contrato de tecnologías de la información y de 60 meses considerados en la aludida licitación, y teniendo presente la necesidad apremiante de implementación en tiempos sumamente ajustados para que se cumpla con la continuidad de servicios, se recibió una oferta de la empresa NETICS SPA, para la prestación de los Servicios de Plataforma de Seguridad y Control Perimetral de INDAP.

25.- Que, entendiéndose configurados los supuestos de trato directo indicado en los Considerando precedente, se suscribió con dicha empresa un contrato para la prestación de Servicios de Plataforma de Seguridad y Control Perimetral de INDAP que incluye servicios de Data Center, que prevé una vigencia que terminará en 24 meses luego de la fecha de inicio de los servicios y/o que terminará junto con la total tramitación del contrato derivado de un eventual proceso futuro de licitación que tenga el mismo objeto y fin de los servicios que se contratan, lo que ocurra primero, y por un monto de UF 29.807,52 (veintinueve mil ochocientos siete coma cincuenta y dos Unidades de Fomento), más IVA.

26.- Que, dicha empresa se encuentra hábil en el portal de compras públicas y se verifico que los servicios en cuestión no están disponibles en convenio marco ni en la plataforma de economía circular

27.-Que, para efectos de garantizar el fiel y oportuno cumplimiento de la contratación, el prestador hizo entrega al Instituto de un Certificado de Fianza Nominativo, a la Vista, Irrevocable Ley N° 20.179, Folio N° 210694WEB, de fecha 13.06.2025, emitido por la Sociedad FINFAST S.A.G.R, por un monto de UF 1.735,00, y una vigencia hasta 09.11.2027.

28.- Que, existe disponibilidad presupuestaria para la contratación de la especie.

29.- Que, la personería del representante del prestador consta en escritura pública de Modificación de Sociedad de fecha 14 de marzo de 2025 suscrita ante don Christian Alejandro Ortíz Cáceres, Notario Público interino de la Séptima Notaría de Santiago, y anotada bajo el repertorio N°2.305-2025.

30.- Que, en la especie se elaboraron los informes del artículo 35 bis de la Ley 19.886 y 80 del Reglamento de Compras Públicas.

31.- Que, en razón del monto de la contratación corresponde que el presente acto sea sometido al control de juridicidad de Contraloría General de la República.

RESUELVO:

1.-Autorízase la modalidad de trato directo con el prestador **NETICS SPA,** RUT N° 76.363.873-1, para la contratación de los Servicios de Plataforma de Seguridad y Control Perimetral de INDAP, lo anterior conforme a lo establecido en el artículo 8 bis, literal c) de la ley de la Ley 19.886, en relación con el artículo 71 N° 3, del Decreto Supremo N° 661 de 2024, del Ministerio de Hacienda, que establece que, la procedencia de trato directo, en casos de emergencia, urgencia o imprevisto, calificados mediante resolución fundada del jefe superior de la entidad contratante, y en virtud de las Consideraciones efectuadas en el presente acto administrativo.

2.- Apruébase el instrumento denominado: "CONTRATO DE PRESTACIÓN DE SERVICIOS DE COMUNICACIONES INSTITUCIONALES DE INDAP", suscrito entre el Instituto de Desarrollo Agropecuario (INDAP) y el prestador **NETICS SPA,** RUT N° 76.363.873-1.

3.- Déjese establecido que de conformidad a la cláusula tercero del contrato, el mencionado instrumento prevé una vigencia que terminará en 24 meses luego de la fecha de inicio de los servicios y/o que terminará junto con la total tramitación del contrato derivado de un eventual proceso futuro de licitación que tenga el mismo objeto y fin de los servicios que se contratan, lo que ocurra primero, y por un monto de UF 29.807,52 (veintinueve mil ochocientos siete coma cincuenta y dos Unidades de Fomento), más IVA, y que, no obstante lo anterior, no podrá cursarse ningún pago relacionado con el presente contrato hasta que la presente resolución se encuentre totalmente tramitada.

4.- Déjese establecido que el monto de la contratación que se aprueba en virtud del presente acto, corresponde a la suma de UF 29.807,52 (veintinueve mil ochocientos siete coma cincuenta y dos Unidades de Fomento), más IVA.

5.-Déjese establecido que el precio de los servicios se pagará conforme a lo indicado en la cláusula cuarta del contrato que se aprueba por este acto.

6.- Impútese el gasto al Subtítulo 22, Ítem 05, Asignación 999, del presupuesto del Instituto de Desarrollo Agropecuario para el año 2025 y con cargo a los recursos que al efecto consulten las respectivas leyes anuales del presupuesto del sector público correspondiente, en el entendido que exista la correspondiente disponibilidad de recursos y se cumpla con las condiciones establecidas para su pago.

7.- Déjese establecido que, para efectos de garantizar el fiel y opo[illegible]miento de la contratación, el prestador hizo entrega al Instituto de un Certificado de Fianza Nominativo, Irrevocable Ley N° 20.179, Folio N° 210694WEB, de fecha 13.06.2025, emitido por la Sociedad FINFAS[illegible] por un monto de UF 1.735,00, y una

vigencia hasta 09.11.2027.

8.- Cúmplese con lo establecido por la Contraloría General de la República, en cuanto se transcribe el texto íntegro del contrato que por medio del presente acto se aprueba:

CONTRATO DE PRESTACIÓN DE SERVICIOS DE PLATAFORMA DE SEGURIDAD Y CONTROL PERIMETRAL DE INDAP
ENTRE
INSTITUTO DE DESARROLLO AGROPECUARIO
Y
NETICS SPA

En Santiago, a 13 de junio de 2025, entre el **INSTITUTO DE DESARROLLO AGROPECUARIO**, servicio público funcionalmente descentralizado del Estado, **RUT N° 61.307.000-1**, en adelante INDAP, representado por su Directora Nacional (S) doña **MARIA ALEJANDRA SANCHEZ CORNEJO**, chilena, cédula de identidad Nº 13.202.795-1, ambos domiciliados para estos efectos en calle Agustinas N° 1465, comuna de Santiago, Región Metropolitana, por una parte y por la otra, la empresa **NETICS SPA,** RUT N° 76.363.873-1, en adelante la empresa, representada legalmente por doña **MELISSA JOHANNA SANHUEZA LARCÓN**, Rut 17.942.250-6 todos domiciliados para estos efectos en Morandé 835, oficina 1713, Santiago, región Metropolitana, se ha convenido celebrar el siguiente contrato de prestación de servicios:

PRIMERO: ANTECEDENTES.

Este Instituto de Desarrollo Agropecuario, requiere contratar servicios de SEGURIDAD Y CONTROL PERIMETRAL DE INDAP, los que contemplan, la adquisición de equipamiento para implementar y habilitar un sistema de enlace SD-WAN para su implementación a nivel nacional.

SEGUNDO: OBJETO DE LA CONTRATACIÓN.

Por el presente acto, INDAP contrata a la empresa para la prestación de los servicios de SEGURIDAD Y CONTROL PERIMETRAL DE INDAP Y SERVICIO DATACENTER, cuyas características se detallan en el Anexo Técnico, el cual forma parte integrante del presente contrato al igual que: La “Oferta Técnica” y “Oferta Económica” presentados por el prestador.

Por su parte, la empresa acepta expresamente cumplir con todas las obligaciones establecidas en el presente contrato, y en su propuesta presentada, todo lo cual forma parte integrante del presente instrumento.

TERCERO: VIGENCIA DEL CONTRATO

La vigencia del contrato se iniciará a contar de la total tramitación de la resolución que lo apruebe. Sin perjuicio de lo anterior, en razón de la naturaleza indispensable de los servicios, aquellos podrán prestarse a contar de la fecha de suscripción del contrato, sin perjuicio de lo anterior, no se realizará ningún pago mientras la resolución que apruebe el contrato no se encuentre totalmente tramitada, es decir notificada al prestador, mediante su publicación en el Sistema de Información (www.mercadopúblico.cl). En virtud de lo anterior, el contrato tendrá una vigencia que terminará en 24 meses contados desde el inicio de la efectiva prestación de los servicios y/o terminará junto con la total tramitación del contrato derivado de un eventual proceso futuro de licitación que tenga el mismo objeto y fin de los servicios que se contratan.

CUARTO: PRECIO Y FORMA DE PAGO

INDAP se compromete a pagar a la empresa un monto total de UF 29.807,52 (veintinueve mil ochocientos siete coma cincuenta y dos Unidades de Fomento), más IVA, los cuales serán pagados en 24 cuotas mensuales de UF 1.214,98 (mil doscientos catorce coma noventa y ocho Unidades de Fomento) más IVA, previa aprobación de la contraparte técnica de INDAP, quien deberá corroborar el cumplimiento tanto de lo especificado en el presente contrato, como de las obligaciones laborales y previsionales que correspondan respecto de los trabajadores del contratante.

El precio corresponde a la oferta económica indicada por el prestador en su oferta económica y forma parte del presente contrato como ANEXO.

Una vez autorizado el pago por la contraparte técnica de INDAP, ésta procederá a señalar al Departamento de Gestión de Abastecimiento que se puede hacer la recepción conforme de los servicios, para posteriormente indicar al oferente seleccionado que puede emitir y enviar el documento electrónico de cobro correspondiente, de manera de proceder al pago respectivo.

La empresa deberá remitir la factura junto a su archivo xml a la casilla de correo dipresrecepcion@custodium.com.

El pago será efectuado por parte de la Tesorería General de la República, y se realizará preferentemente a través de transferencia electrónica, para lo cual el oferente deberá enviar por única vez, un correo electrónico a la casilla contabilidad@indap.cl, señalando los antecedentes para efectuar la operación, tales como: número de cuenta corriente, Banco, RUT, razón social, mail y número telefónico de la persona encargada de recibir el comprobante de transferencia. En caso de que no se envíen los antecedentes bancarios, el pago se realizará con cheque, el que se enviará por carta certificada a la dirección inscrita en servicios de impuestos internos.

QUINTO: GARANTÍA DE FIEL CUMPLIMIENTO DE CONTRATO

Junto con la suscripción del presente instrumento, la empresa hizo entrega a favor de INDAP de una garantía de fiel cumplimiento de contrato, equivalente a un 5% del precio final neto ofertado, la que deberá mantenerse vigente, en forma permanente, al menos por 60 (sesenta) días hábiles posteriores a la fecha establecida para el término del contrato.

La garantía será devuelta, si procediere, con posterioridad al término del servicio, previo cumplimiento de las obligaciones contractuales y extracontractuales entre las partes.

Todo gasto que irrogue la mantención de la garantía será de cargo de la empresa, quien será responsable de realizar los trámites para mantenerla vigente por el período que cauciona. La ga[illegible]á ser renovada en caso de prórroga o renovación del contrato; el no cumplimiento de este trámite será m[illegible]ue INDAP ponga término anticipado al contrato.

INDAP podrá efectuar el cobro de la garantía de fiel cumplimiento d[illegible] mediante acto administrativo fundado y

debidamente tramitado, por las causales indicadas en la cláusula octava del presente contrato, haya procedido o no el término anticipado de contrato.

SEXTO: DE LA CESIÓN Y SUBCONTRATACIÓN

La empresa no podrá ceder ni transferir en forma alguna, total ni parcialmente, los derechos y obligaciones que nacen del presente contrato.

El prestador podrá concertar con terceros la subcontratación parcial de los servicios contratados, en los términos establecidos en los artículos 183-A y siguientes del Código del Trabajo. El prestador solo podrá subcontratar servicios en forma parcial, sin perjuicio que la responsabilidad de su cumplimiento permanecerá en el prestador.

Conforme a lo previsto en el artículo 128 del Reglamento de Compras Públicas, el prestador podrá concertar con terceros la subcontratación parcial del contrato, sin perjuicio que la responsabilidad de su cumplimiento permanecerá en el prestador principal.

El oferente a más tardar, cuando inicie la ejecución del contrato, deberá informar a la Contraparte Técnica de INDAP, la parte del contrato que tenga previsto subcontratar, su importe y el nombre o razón social del subcontratista hábil en el Registro de Proveedores.

Se deja establecido que no será admisible la subcontratación en los siguientes casos:

a) Si se trata de servicios especiales, y se ha contratado en vista de la capacidad o idoneidad del contratista.
b) Si excede el treinta por ciento del monto total del contrato.
c) Si afecta al subcontratista una o más causales de inhabilidad en el Registro de Proveedores.
d) Si el subcontratista se encuentra en alguna de las incompatibilidades para ser contratado por la Entidad pública a que se refiere el artículo 35 quáter de la Ley de Compras.

El prestador principal deberá notificar por escrito a INDAP de cualquier modificación en las prestaciones que deberá desarrollar el subcontratista, o en su identidad, con anterioridad a la materialización de estos cambios, cuestión que debe ser aprobada por la Contraparte Técnica de INDAP. En caso de un cambio en la identidad de un subcontratista, el prestador principal deberá acreditar que este cumple con los requisitos señalados y aquello debe ser aprobado por INDAP.

El límite de la subcontratación no podrá exceder el 30% del contrato, y en ningún caso la subcontratación podrá ser utilizada para efectuar una cesión del contrato.

INDAP no será solidariamente responsable de las obligaciones laborales y previsionales de dar que afecten a los contratistas en favor de los trabajadores de éstos, incluidas las eventuales indemnizaciones legales que correspondan por término de la relación laboral, ya que INDAP hará ejercicio de los derechos de información y retención que le otorga la Ley N° 20.123/2006. Por lo anterior, el contratista tendrá la obligación de informar a INDAP sobre el monto y estado de cumplimiento de las obligaciones laborales y previsionales que correspondan respecto a sus trabajadores, previo requerimiento de INDAP. El monto y estado de cumplimiento de dichas obligaciones laborales y previsionales deberá ser acreditado mediante certificados emitidos por la respectiva Inspección del Trabajo, o bien por medios idóneos que garanticen la veracidad de dicho monto y estado de cumplimiento, de acuerdo con lo establecido por el Ministerio del Trabajo y Previsión Social.

En el caso de que el prestador no acredite oportunamente el cumplimiento íntegro de las obligaciones laborales y previsionales en la forma señalada, INDAP podrá retener de las obligaciones que tenga a favor del contratista, el monto de que es responsable, debiendo pagar con esta retención a los trabajadores o institución previsional acreedora, de acuerdo con lo dispuesto en el artículo 183-C del Código del Trabajo. De la misma forma, en caso de incumplimiento del prestador de las obligaciones laborales o sociales con sus trabajadores, INDAP estará facultado para hacer efectiva la garantía de cumplimiento, administrativamente y sin necesidad de requerimiento ni acción judicial o arbitral alguna, según lo establece el artículo 124 del Reglamento de la Ley N° 19.886.

El personal de la empresa que ejecute los servicios dependerá única y exclusivamente del oferente prestador y, por lo tanto, no tendrá relación laboral directa o indirecta con el Instituto de Desarrollo Agropecuario, ni con ninguna de sus dependencias. Asimismo, INDAP no se responsabilizará de ningún accidente, enfermedad, pérdida o daño que pueda presentarse en el personal de la empresa que puedan concurrir a las dependencias de INDAP durante la ejecución de los servicios, ya que el prestador se obliga a cumplir, en relación con sus trabajadores, con todas las normas de higiene y seguridad en el trabajo a que se refiere la Ley N° 16.744 sobre Accidentes del Trabajo y Enfermedades Profesionales.

SÉPTIMO: MODIFICACIONES AL CONTRATO

Conforme a lo establecido en el Artículo 13 de la Ley N° 19.886 y lo señalado en el artículo 129 del Decreto Supremo 661 del Ministerio de Hacienda, que contiene el Reglamento de la Ley de Compras, y considerando la envergadura del contrato y la posibilidad de que, producto de las políticas del Instituto y de otros múltiples factores, varíen las actuales necesidades, se establece expresamente la posibilidad de modificar el contrato de común acuerdo durante su vigencia, aumentando y/o disminuyendo hasta en un 30%, cualquiera de los aspectos esencialmente variables contenidos en la presente contratación, esto es:

1. El monto contratado
2. El plazo del contrato
3. Otros servicios no previstos inicialmente conforme a lo dispuesto en el artículo 129 numeral 2 del Reglamento de Compras Públicas y únicamente cuando se verifique que sean indispensables para la continuidad operativa del servicio.

Lo anterior, siempre y cuando se cuente con disponibilidad presupuestaria para ello.

En tales circunstancias, las partes se comprometen, en relación con dichas variaciones, a efectuar las respectivas adecuaciones de los servicios en base al concepto de estricta proporcionalidad, manteniendo vigentes todas las demás condiciones del contrato, velándose por el cumplimiento de los principios de estricta sujeción a las bases, igualdad de los oferentes y el equilibrio financiero del contrato. Dicha modificación debe ser aprobada mediante el acto administrativo respectivo.

OCTAVO: SANCIONES POR INCUMPLIMIENTO.

1.-TÉRMINO ANTICIPADO DE CONTRATO.

El contrato, ya sea que este se haya consagrado en un documento suscrito por ambas partes o por la sola emisión de la orden de compra, podrá terminarse anticipadamente, de conformidad a lo establecido en el artículo 13 de la Ley N° 19.886 y el artículo 130 del Reglamento de la Ley N° 19.886, por las siguientes causas:

A) La muerte o incapacidad sobreviniente de la persona natural, o la extinción de la personalidad jurídica de la sociedad contratista.
B) La resciliación o mutuo acuerdo entre las partes, siempre que el Proveedor no se encuentre en mora de cumplir sus obligaciones. Para efectos de terminar anticipadamente el contrato por la causal prevista en este literal, las partes deberán suscribir un instrumento que dé cuenta del término anticipado de mutuo acuerdo y las razones que lo motivaron el que deberá ser aprobado mediante el respectivo acto administrativo, debiendo además establecer, si correspondiere, el monto que INDAP deba pagar al contratante por los servicios efectivamente prestados hasta antes de la causal que le pone término al contrato, así como los productos o documentos que el contratante deba entregar a INDAP.
C) El incumplimiento grave de las obligaciones contraídas por el Proveedor. Este Instituto entiende como incumplimiento grave las siguientes:

1. La negativa, sin causa justificada, de prestar cualquiera de los servicios a los que se hubiere comprometido en su oferta.
2. Aplicación de multas por un total acumulado equivalente al 30% del valor del contrato.
3. Aplicación de multas superando los topes establecidos para cada una de ellas, esto es exceder los 10 días hábiles de atraso o incumplir 5 obligaciones durante la vigencia del contrato.
4. No pago de las multas debidamente cursadas en el plazo establecido.
5. No renovar la garantía de fiel y oportuno cumplimiento en caso de renovación o prórroga del contrato.
6. No reponer la garantía de fiel y oportuno cumplimiento en caso de cobro de esta.
7. Transgredir la prohibición de subcontratar, ceder, traspasar y/o transferir, total o parcialmente, a cualquier título, los derechos y obligaciones que se establezcan en el contrato.
8. **Para el caso de las UTP**, adicionalmente a las acciones precedentes, configuran incumplimiento grave de las obligaciones contraídas las siguientes: - La constatación de que los integrantes de la UTP constituyeron dicha figura con el objeto de vulnerar la libre competencia. De verificarse tal circunstancia, se remitirán los antecedentes pertinentes a la Fiscalía Nacional Económica. - Si uno de los integrantes de la UTP se retira de ésta, y dicho integrante reuniese una o más características objeto de evaluación de la oferta. - Ocultar información relevante para ejecutar el contrato, que afecte a cualquiera de sus miembros. - Inhabilidad sobreviniente de alguno de sus integrantes, en la medida que la UTP no pueda continuar ejecutando el contrato con los restantes miembros, en los mismos términos contratados. - Disolución de la UTP.

D) El estado de notoria insolvencia del contratante, a menos que se mejoren las cauciones entregadas o las existentes sean suficientes para garantizar el cumplimiento del contrato.
E) La imposibilidad de ejecutar la prestación en los términos inicialmente pactados, cuando no sea posible modificar el contrato conforme al artículo 129 precedente. En tal caso, la Entidad sólo pagará el precio por los bienes y/o servicios que efectivamente se hubieren entregado o prestado, según corresponda, durante la vigencia del contrato. Asimismo, en el evento que la imposibilidad de cumplimiento del contrato obedeciere a motivos imputables al Proveedor, procederá que se apliquen en su contra las medidas establecidas en el artículo 135 de este reglamento
F) Por exigirlo el interés público o la seguridad nacional.
G) Las demás que se establezcan en el contrato; estableciéndose en el presente contrato las siguientes causas que pudieran ocurrir o revelarse durante toda la vigencia del contrato.
1.Si el contratante perdiere las certificaciones y autorizaciones necesarias para funcionar en el giro de su actividad, decretada por autoridad competente.
2. Haber sido condenado el contratante por crimen o simple delito.
3. Haber sido condenado el contratante, como consecuencia de incumplimiento de un contrato celebrado con alguna entidad 4. regida por la Ley N° 19.886, y siempre que no hayan transcurrido dos años a contar desde la fecha de la sentencia.
5. Haber sido suspendido el contratante o haber sido eliminado del Registro de Proveedores, a través de una resolución fundada de la Dirección de Compras Públicas.
6. Si el contratante se encontrara en Estado Inhábil para suscribir contratos con Organismos Públicos del Estado, de acuerdo con el reporte entregado por el Registro de Proveedores de Mercado Público.
7. Si los resultados obtenidos de la prestación de los servicios no son los esperados, por lo que continuar con su desarrollo perjudica a INDAP.

El término anticipado de contrato por cualquiera de las causales aquí establecidas deberá ser formalizado mediante acto administrativo fundado, debidamente tramitado, el que deberá establecer, si correspondiere, el monto que INDAP deba pagar al contratante por los servicios efectivamente prestados hasta antes de la causal que le pone término al contrato, así como los productos o documentos que el contratante deba entregar a INDAP.

Lo establecido en este numeral es sin perjuicio de las acciones que INDAP pueda ejercer para exigir el cumplimiento forzado de lo pactado o la resolución del contrato, en ambos casos, con la correspondiente indemnización de perjuicios.

Con excepción de las causales contempladas en las letras b) y f) precedentes, en los supuestos de caso fortuito o fuerza mayor que por razones de ley o acto de autoridad hagan imperiosa e [illegible] y ello sea calificado así por el Instituto, una vez adoptada aquella, el Instituto procederá a hacer efectiva la ga[illegible]el y oportuno cumplimiento del contrato,

sin perjuicio de ejercer las demás acciones que procedan, especialmente la indemnizatoria de los perjuicios causados. INDAP podrá dar cuenta de tales hechos a la Dirección de Compras y Contratación Pública, para los efectos de que el contratante sea suspendido o eliminado, según corresponda, del Registro Electrónico Oficial de Proveedores de la Administración, de conformidad a los artículos 154°, 159°, 160° y 162° del Reglamento de la Ley N° 19.886.

Fuerza mayor y caso fortuito

- Las partes no serán responsables en caso de incumplimiento tardío de las obligaciones contractuales debido a hechos independientes de su voluntad, considerados como fuerza mayor o caso fortuito, en los términos señalados en el artículo 45 del Código Civil de Chile.
- Si el oferente seleccionado se ve impedido de cumplir con sus obligaciones contractuales por un evento considerado caso fortuito o fuerza mayor, deberá notificar de ese hecho a INDAP por escrito y en un plazo no superior a cinco (5) días hábiles desde iniciado u ocurrido el hecho que lo ocasiona, y solicitar prórroga para el cumplimiento de la obligación afectada.
- La notificación de solicitud de prórroga deberá presentarse acompañada de un informe en el que consten los hechos considerados caso fortuito o fuerza mayor, los cuales deberán estar debidamente fundados, indicando la incidencia que dicha situación tendría en el cumplimiento de los plazos establecidos.
- La calificación de la fuerza mayor o caso fortuito será resuelta por INDAP, mediante resolución fundada sobre la base de los antecedentes que, oportunamente, le proporcione el oferente seleccionado y/o aquellos otros que obtenga de terceros, o sean de conocimiento público.
- En cualquier caso, si el oferente seleccionado no pudiere cumplir con sus obligaciones, procurará atenuar los daños y cumplirá con ellas tan pronto como finalicen los hechos que dieron lugar al caso fortuito o a la causa de fuerza mayor.
- Si la causa de caso fortuito o fuerza mayor impidiera al oferente seleccionado cumplir con las obligaciones asumidas por más de treinta (30) días, el contrato se resolverá de pleno derecho.
- Para efectos de terminar anticipadamente el contrato por fuerza mayor o caso fortuito, se aplicará previamente el Procedimiento sancionatorio previsto en el presente contrato.

2.-MULTAS:

INDAP podrá cobrar multas al contratante, administrativamente, cuando éste no cumpla con lo estipulado en el contrato, siempre que se deba a causa imputable al contratante, en los siguientes términos:

A. NIVELES DE SERVICIO Y REPOSICIÓN DE EQUIPOS: De acuerdo con lo establecido en el Anexo Técnico que señalan los niveles de servicio, INDAP procederá a cobrar multas a la empresa, administrativamente, cuando éste no cumpla con lo estipulado en dichas tablas y/o en el presente contrato, siempre que se deba a causa imputable la empresa, las que se aplicarán en los términos detallados en las referidas tablas del Anexo Técnico respectivo, que forman parte integrante del presente contrato.
B.- Incumplimiento de otras obligaciones distintas a plazo previstas en las bases técnicas que no digan relación con el plazo un monto de UF 20 por cada infracción.
C.-El incumplimiento de los plazos y/o fechas que se fijen para la ejecución de las actividades y procesos asociados a los servicios, será sancionado con el valor de UF 20 por cada día hábil de atraso.

En cualquier caso, las multas no podrán superar el 30% del monto total del contrato.

PAGO DE LAS MULTAS:

1. El pago de las multas que correspondan deberá ser efectuado dentro de los cinco (5) días hábiles siguientes a la notificación de la resolución que aplica la multa, mediante una transferencia electrónica o algún otro medio de pago que se determine.
2. En caso que el contratante no pague la multa dentro del plazo establecido, facultará a INDAP para descontar el monto adeudado del estado de pago pendiente y/o para proceder al cobro de la garantía de fiel y oportuno cumplimiento de contrato y/o para terminar anticipadamente el contrato, a elección de INDAP.
3. Se hace presente que contra la resolución que aplica la multa, proceden los recursos consagrados en la Ley N° 19.880, los que deberán interponerse dentro de los plazos legales, ante el Director Nacional de INDAP, sin perjuicio de que el contratante pueda ejercitar cualquier otro recurso que estime oportuno.
4. Para todos los efectos de la aplicación de lo dispuesto en este punto, el valor de la Unidad de Fomento será el correspondiente a la fecha de su efectiva aplicación.
5. El tope máximo de las multas será del 30% del valor del contrato.
6. En caso que se aplique multa y ésta se haga efectiva en la garantía de fiel cumplimiento, el prestador deberá reemplazar dicha garantía por una igual a la establecida en este contrato.
7. Ejecutada la garantía, el Instituto descontará de la misma el monto de la multa y devolverá el saldo al Prestador solo una vez que éste entregue la garantía de reemplazo.

Si excediese los 10 días hábiles de atraso o incumpliera 5 obligaciones durante la vigencia del contrato, INDAP quedará facultado para poner término anticipado al contrato y/o hacer efectivo el instrumento financiero de garantía de fiel y oportuno cumplimiento de contrato, sin perjuicio del cobro de las multas, de acuerdo al Procedimiento para la aplicación de sanciones que se establece a continuación.

NOVENO: PROCEDIMIENTO SANCIONATORIO (MULTAS Y TERMINO ANTICIPADO)

INDAP notificará al contratante mediante correo electrónico dirigido a la casilla electrónica que indicada en la identificación del proponente adjunta a este contrato o en su defecto en la que tenga registrado en el Sistema de Información de la Dirección de Compras y Contratación Pública, www.mercadopublico.cl y/o en el Registro de Proveedores, la intención de cursar una multa o término anticipado de contrato, según corresponda mediante correo electrónico, indicando la causal de que se trata e indicando que el prestador tiene un plazo de 5 días para deducir sus descargos si procediere.

El contratante podrá reclamar o presentar sus descargos a INDAP, dentro del quinto (5°) día hábil contado desde la notificación anteriormente indicada, mediante solicitud escrita enviada a través de correo electrónico a la dirección abastecimiento@indap.cl, la que deberá ser fundada.

INDAP resolverá la reclamación presentada por el contratante dentro del decimoquinto (15°) día hábil, acogiendo los fundamentos presentados, o bien rechazándolos y dando por terminado el contrato, lo que deberá ser aprobado mediante acto administrativo fundado, debidamente tramitado, y posteriormente notificado al contratante mediante correo electrónico, adjuntando la resolución fundada correspondiente.

Se hace presente que contra la resolución que aplica la sanción, proceden los recursos consagrados en la Ley N° 19.880, los que deberán interponerse dentro de los plazos legales, ante el Director Nacional de INDAP, sin perjuicio de que el contratante pueda ejercitar cualquier otro recurso que estime oportuno.

En los casos de término anticipado por resciliación o mutuo acuerdo entre las partes no regirá este procedimiento sin perjuicio de que deberá suscribirse un instrumento que dé cuenta de dicho acuerdo, el que deberá ser aprobado mediante el respectivo acto administrativo.

DÉCIMO: CONTRAPARTE DE INDAP

INDAP se relacionará con la empresa, tanto en los aspectos técnicos como operacionales y administrativos, con una Contraparte Técnica que se designará para tales efectos, para efectuar las siguientes tareas y funciones:

- Supervisar y controlar el desarrollo de los servicios contratados, velando por el estricto cumplimiento de sus objetivos y de los plazos acordados para su ejecución.
- Analizar el avance y resultados de las diferentes actividades, revisando y aprobando los servicios, planteando al contratante las observaciones y/o recomendaciones que se estimen pertinentes.
- Resolver cualquier problema o situación no prevista de acuerdo con los criterios y determinaciones estipuladas por INDAP.
- Colaborar con el contratante en el ámbito de sus competencias, poniendo a su disposición lo necesario para la buena ejecución del contrato.
- Autorizar los pagos a la empresa, debiendo corroborar el cumplimiento tanto de lo establecido en el presente contrato, como de las obligaciones laborales y previsionales que correspondan respecto de los trabajadores de la empresa.

DÉCIMOPRIMERO: SEGURIDAD DE LA INFORMACIÓN

Acceso a la Información: la empresa solo tendrá acceso a la información institucional relevante que sea necesaria para prestar el servicio para el que ha sido contratado, lo que será determinado y documentado por el Encargado de Seguridad de la Información Institucional.

Obligaciones y confidencialidad: por este acto, la empresa se obliga a cumplir la normativa de seguridad de la información de INDAP, de acuerdo con las políticas y procedimientos establecidos, incluida la Resolución Exenta N° 000417, de 2012, de la Dirección Nacional, que aprueba la Política de Seguridad de la Información Institucional y la Resolución Exenta N° 140417, de 2012, de la Dirección Nacional, que Establece infracciones al Sistema de Seguridad de la Información. Asimismo, la empresa se obliga a mantener la confidencialidad de la información personal que pueda llegar a conocer sobre los funcionarios o beneficiarios de INDAP, así como también de procedimientos, ideas, productos, servicios, procesos y nombres de personas, instituciones y empresas que utilizan los productos y servicios de INDAP. De esta forma, la empresa no podrá, sin el consentimiento expreso manifestado por escrito por INDAP, usar para el beneficio propio o de cualquier otra persona, empresa o corporación, divulgar, publicar o comunicar cualquier secreto o información confidencial, que pudo haber adquirido o pueda adquirir o conocer en razón de este contrato.

No divulgación: además de las obligaciones que emanan de la naturaleza del contrato del que da cuenta el presente instrumento, la empresa estará obligado a mantener la información confidencial en estricta reserva y no revelar ningún dato de la información, relacionada o no, sin el consentimiento previo y escrito de INDAP. Para ello, la empresa se obliga a instruir al personal que estará encargado de recibir la información confidencial de propiedad de INDAP, debiendo suscribir el correspondiente acuerdo de confidencialidad si fuere necesario, de su obligación de recibir, tratar y usar la información que reciban como confidencial y destinarla únicamente al propósito objeto del contrato, en los mismos términos en que se establece en el presente instrumento. Asimismo, la empresa se obliga a divulgar la información confidencial únicamente a las personas autorizadas para su recepción dentro de la organización; a tratar confidencialmente toda la información recibida directa o indirectamente de INDAP, y no utilizar ningún dato a un objeto distinto del contrato; y no manejar, usar, explotar, o divulgar la información confidencial a ninguna persona o entidad por ningún motivo en contravención a lo dispuesto en este instrumento.

Protección de Datos Personales: la empresa, de acuerdo a lo establecido en la Ley N° 19628, deberá dar estricto cumplimiento a las leyes sobre protección de datos de carácter personal, asegurando su confidencialidad, obligándose por este acto, a no transferirlos o cederlos, salvo en aquellos casos en que la legislación vigente así lo indique.

Auditoría y Supervisión: INDAP, en caso de ser necesario, se faculta para auditar los procesos y servicios que el proveedor se obliga a realizar por este acto. La responsabilidad de administrar las relaciones con la empresa se asigna al Encargado de Seguridad de la Información Institucional, quien debe monitorear y revisar regularmente los servicios definidos en el presente contrato. El monitoreo y revisión de los servicios debe garantizar que los términos y condiciones de seguridad de la información se respeten y que los incidentes y problemas de seguridad de la información se gestionen correctamente. En caso de observarse deficiencias en la prestación de los servicios, se deben tomar las medidas necesarias para corregir el problema. En caso de subsistir, será una causal de término anticipado del contrato.

Gestión de Cambios: En caso de que las partes determinen realizar cambios en la provisión de servicios por parte de la empresa, se deberán mantener o mejorar las políticas de seguridad de la información, así como los procedimientos y

controles específicos, considerando la criticidad de la información del negocio, los sistemas y procesos involucrados y la reevaluación de los riesgos.

DÉCIMOSEGUNDO: PROPIEDAD INTELECTUAL

Se entenderá por "Propiedad Intelectual" todos aquellos procedimientos o métodos de elaboración, inventos o descubrimientos, patentes, modelos, diseños y dibujos industriales, secretos industriales o comerciales, nombres de dominio, obras, programas computacionales, datos, bases de datos, conocimientos, know-how, marcas comerciales y signos distintivos y, en general, cualquier bien material o inmaterial y/o derechos e intereses relacionados con la creación intelectual, estén o no protegidos bajo las leyes de propiedad intelectual y/o industrial.

La empresa no podrá publicar, reproducir, adaptar, ejecutar o comunicar públicamente, comercializar, descompilar, manipular, entregar a terceros y/o utilizar o explotar la Propiedad Intelectual de INDAP, sino en los términos y en las condiciones que al efecto se han establecido por este instrumento. Las partes acuerdan expresamente que la totalidad de los derechos de propiedad intelectual sobre toda recomendación, idea, técnica, know- how, diseño, metodología, software desarrollado por o para INDAP u otra información técnica, sobre el producto final o de alguna de sus etapas de desarrollo, corresponden a INDAP.

Asimismo, toda información que se genere como parte de la prestación de servicios de implantación, será propiedad de INDAP. Toda la documentación que se genere como parte de la prestación de servicios, ya sea en formato Microsoft Word, PowerPoint, Excel, Project, Adobe PDF, etc., deberá presentarse exclusivamente con la imagen corporativa de INDAP.

Finalmente, la empresa se obliga a no inscribir a su nombre cualquier proceso, etapa, proyecto o producto originado con ocasión o a causa del servicio contratado en cualquier Registro del país.

DÉCIMOTERCERO: LEGISLACIÓN APLICABLE Y JURISDICCIÓN

El presente contrato queda sujeto a la legislación civil chilena y para todos sus efectos las partes se someten, en lo que fuera procedente, ante cualquier controversia, a la jurisdicción de los Tribunales Ordinarios de Justicia con asiento en la comuna y ciudad de Santiago.

DECIMOCUARTO: ORDEN DE PRELACIÓN.

En caso de existir algún aparente inconveniente o se viere alguna contradicción en los instrumentos que regulan la presente contratación, se declara que legalmente el orden de prelación normativo es el siguiente:

1.- Ley Nº 19.886 y su reglamento.
2.- El presente Contrato.
3.- Oferta del prestador.

DÉCIMOQUINTO: EJEMPLARES

El presente contrato se firma en dos (2) ejemplares del mismo tenor y fecha, quedando uno de ellos en poder de INDAP y otro en poder de la empresa.

DÉCIMOSEXTO:PERSONERÍAS

La personería de don(ña) MARIA ALEJANDRA SANCHEZ CORNEJO para representar al INSTITUTO DE DESARROLLO AGROPECUARIO, consta en el Decreto Exento N° 64 de 03 de mayo de 2023 del Ministerio de Agricultura.

La personería de doña **MELISSA JOHANNA SANHUEZA LARCÓN** para representar legalmente a la empresa NETICS SPA, consta en escritura pública de 14 de marzo de 2025 suscrita ante don Christian Alejandro Ortíz Cáceres, Notario Público interino de la Séptima Notaría de Santiago, y anotada bajo el repertorio N°2.305-2025.

MARIA ALEJANDRA SANCHEZ CORNEJO	**MELISSA JOHANNA SANHUEZA LARCÓN**
DIRECTORA NACIONAL (S)	**REPRESENTANTE**
INSTITUTO DE DESARROLLO AGROPECUARIO	NETICS SPA.

ANEXO TÉCNICO

I.- OBJETO DE LA CONTRATACIÓN.

Este Instituto de Desarrollo Agropecuario, requiere contratar servicios de SEGURIDAD Y CONTROL PERIMETRAL DE INDAP Y SERVICIO DATACENTER, los que contemplan, la adquisición de equipamiento para implementar y habilitar un sistema de enlace SD-WAN para su implementación a nivel nacional. Todo lo anterior, a objeto de acceder a una solución integral para mejorar las condiciones de conectividad institucional, satisfaciendo así las necesidades existentes en esta materia. El objetivo esencial que se propone con este proyecto es optimizar la plataforma de comunicaciones institucional, a fin de dar plena cobertura a los actuales requerimientos de INDAP y sus oficinas existentes en las distintas regiones del país, como asimismo permitir la posibilidad de ampliar su capacidad para responder a un potencial crecimiento futuro por mayores necesidades de este servicio. Sin perjuicio de ello lo anterior se enmarca en la necesidad de dar continuidad operacional al servicio dando cumplimiento a los estándares mínimos de seguridad requeridos en la normativa vigente.

II.- COMPONENTES DE LA SOLUCIÓN REQUERIDA.

- El servicio debe constar de provisión, instalación, implementación, puesta en marcha de toda la solución ofertada.
- El servicio debe incluir equipos y accesorios nuevos.
- Todas las licencias, soporte de fabricante y servicios deben estar por 24 meses.
- El servicio debe incluir todos los componentes necesarios para la puesta en operación de la plataforma, (cables de energía, patchcord Fibra Optica/UTP cobre, Ordenamiento de Rack, conectores, transceivers).
- El servicio debe ser realizado por ingenieros especialistas con certificaciones NSE4 y NSE7, los cuales se mantendrán durante la vigencia del contrato.
- Los equipos se entregarán en las dependencias de INDAP con al menos 2 semanas de anterioridad de la fecha definida para la implementación.
- El servicio debe incluir un equipo multidisciplinario para la puesta en marcha de la plataforma implementada, se especifica en el organigrama.
- Los equipos Firewall deben ser configurados en HA solo en [illegible] migrarán (si que existe otro equipo

perimetral) si no, una configuración de cero, y ajustaran las configuraciones: configurar VDOM, politicas, nat, enrutamiento, objetos y todo lo necesario para la correcta instalación y configuracion.

- Posterior a la instalación y configuración (equipamiento), se realizará recomendaciones de mejora a las políticas.
- El servicio debe incluir la optimización de configuraciones, reglas, vpn, integraciones, enrutamiento y adicionales de toda la plataforma ofertada.
- Se incluyen las mantenciones de la plataforma ofertada, la cual incluye actividades de actualización de firmware, patches, y remediaciones publicadas por el fabricante en relación a vulnerabiliades confirmadas.
- Se incluye el servicio post-venta durante la vigencia del contrato en modalidad 24x7x365.
- Se incluye matriz de escalamiento técnico y comercial durante la vigencia del contrato.
- De ser necesario un cambio en los miembros del equipo durante la ejecución del servicio, se informará a INDAP y pueden autorizar el nuevo recurso o solicitar el cambio.
- El servicio incluye el informe mensual de la plataforma ofertada, y se incluye una reunión mensual de seguimiento para implementación de mejoras y revisión del servicio.
- Se incluye una visita trimestral para la revisión física de los equipos, y reunión de forma local de seguimiento del servicio.
- Se incluye todo el etiquetado, ordenamiento y adecuación de los equipos ofertados.
- Los equipos Firewall ofertados deben cumplir en su totalidad con funcionalidades, licencias y soportes requeridos.
- Se debe incluir entrega de conocimientos para los funcionarios que requieran INDAP.
- Se incluye Forticare Premium en toda la plataforma ofertada, lo cual garantiza el reemplazo de partes y piezas en Next Business Day con el servicio Priority Rma (PRMA).
- Se incluye carta gantt del proyecto, la cual puede ser ajustada por la INDAP de acuerdo a sus objetivos.
- Se diseñará un plan de trabajo posterior al levantamiento de información, donde se especificarán las actividades a realizar, metodologías de implementación, proceso de roll back, pruebas de servicios definidos con INDAP, validaciones finales y proceso de marcha blanca.
- Todos los equipos se configurarán de manera offline, para tener la infraestructura preparada para la indisponibilidad de servicio.
- Se adjunta carta Gantt.

CARTA GANTT

Hito	Duración días
Reunión inicial Kick off	1
Entrega de Equipos	10
Levantamiento de información de la infraeestructura actual	5
Diseño y aprobación plan de trabajo entre las partes	5
Mudanza y Aprovisionamiento Datacenter	5
Despliegue e instalación de equipos Fortinet	60
Documentación plataforma	2
Transferencia de conocimiento de plataforma implementada	2
TOTAL DIAS	90

III.- COMPONENTES ESPECÍFICOS.

1.-PRODUCTOS

ITEM	SKU	DESCRIPCION	CANTIDAD	EQUIPO	DURACION
1	FG-400F	FortiGate-400F 18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, 8 x 10GE SFP+ slots, SPU NP7 and CP9 hardware accelerated, dual AC power supplies	2	FIREWALL	N/A
2	FG-120G	FortiGate-120G 18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, 4 x 10GE SFP+ slots, SP5 hardware accelerated, dual AC power supplies	16	FIREWALL	N/A
3	FWF-80F-2R-N	FortiWiFi-80F-2R 8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports, dual WiFi radio. Region Code N	138	FIREWALL	N/A
4	FG-600F	FortiGate-600F 4x 25G SFP28 slots, 4 x 10GE SFP+ slots, 18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, SPU NP7 and CP9 hardware accelerated, dual AC power supplies	2	FIREWALL	N/A

5	FS-1024E	FortiSwitch-1024E Layer 2/3 FortiGate switch controller compatible switch with 24 x GE/10GE SFP/SFP+ slots and 2 x 100GE QSFP28. Dual AC power supplies	5	SWITCH	N/A
6	FS-148F	FortiSwitch-148F FortiSwitch-148F is a performance/price competitive L2+ management switch with 48x GE port + 4x SFP+ port + 1x RJ45 console	1	SWITCH	N/A
7	FS-124F-FPOE	FortiSwitch-124F-FPOE L2+ managed POE switch with 24GE + 4SFP+, 24port POE with max 370W limit and smart fan temperature control	134	SWITCH	N/A
8	FS-148F-FPOE	FortiSwitch-148F-FPOE FortiSwitch-148F-FPOE is a performance/price competitive L2+ management switch with 48x GE port + 4x SFP+ port + 1x RJ45 console. Port 1- 48 are POE ports with automatic Max 740W POE output limit (48 port 802.3af or 24 port 802.3at)	63	SWITCH	N/A
9	FAP-231G-N	FortiAP-231G Indoor Wireless AP - Tri radio (Wi-Fi-6E IEEE 802.11ax Tri-band 2.4/5/6GHz and dual 5G operation 2+2+2 2 streams 3 radios) [Note: 6GHz band not available in all regulatory domains], internal antennas, 1x10/100/1000 RJ45 , 1x 100/1000/2500 Base-T RJ45, BT/BLE, 1x Type A USB, Console Port (RJ45). Ceiling/wall mount kit included. For power order: 802.3at PoE injector GPI-130 or AC adapter SP-FAP200-PA. Region Code N	43	Access Point	N/A
10	FAZ-300G	FortiAnalyzer-300G Centralized log & analysis appliance - 4x GE RJ45, 8TB storage, up to 100GB/Day of logs.	1	FortiAnalyzer	N/A
11	FN-TRAN-SFP+SR	10GE SFP+ transceiver module, short range 10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots	108	Accesorio	N/A
12	FN-TRAN-SFP+GC	10GE copper SFP+ RJ45 Transceiver (30m range) 10GE copper SFP+ RJ45 transceiver module (30m range) for systems with SFP+ slots	680	Accesorio	N/A
13	FN-CABLE-SFP+5	10 GE SFP+ passive direct attach cable, 5m 10 GE SFP+ passive direct attach cable, 5m for systems with SFP+ and SFP/SFP+ slots	5	Accesorio	N/A
14	GPI-130	GPI-130 Gigabit PoE Injector 1-Port Gigabit PoE Power Injector, 802.3at up to 30W for GPI-130 Gigabit PoE Injector	2	Accesorio	N/A
15	FN-TRAN-SFP+SR	10GE SFP+ transceiver module, short range 10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots	1	Accesorio	N/A
16	FN-TRAN-SFP+GC	10GE copper SFP+ RJ45 Transceiver (30m range) 10GE copper SFP+ RJ45 transceiver module (30m range) for systems with SFP+ slots	1	Accesorio	
17	FC-10-0400F-950-02-24	FortiGate-400F x Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)	2	Licencia	24 Meses
18	FC-10-F120G-950-02-24	FortiGate-120G x Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)	16	Licencia	24 Meses
19	FC-10-W080F-950-02-24	FortiWiFi-80F-2R x Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)	138	Licencia	24 Meses
20	FC-10-0600F-950-02-24	FortiGate-600F x Year Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)	2	Licencia	24 Meses
21	FC-10-S1E24-247-02-24	FortiSwitch-1024E x Year FortiCare Premium Support	5	Licencia	24 Meses
22	FS-SW-LIC-1000	FortiSwitch Advanced Features License SW License for FS-1000 Series Switches to activate Advanced Features	4	Licencia	24 Meses
23	FC-10-148FN-247-02-24	FortiSwitch-148F x Year FortiCare Premium Support	1	Licencia	24 Meses
24	FC-10-S124F-247-02-24	FortiSwitch-124F-FPOE x Year FortiCare Premium Support	134	Licencia	24 Meses
25	FC-10-148FF-247-02-24	FortiSwitch-148F-FPOE x Year FortiCare Premium Support		Licencia	24 Meses

26	FC-10-PG231-247-02-24	FortiAP-231G x Year FortiCare Premium Support	43	Licencia	24 Meses
27	FC-10-L03HG-247-02-24	FortiAnalyzer-300G x Year FortiCare Premium Support	1	Licencia	24 Meses
28	FC2-10-MVCLD-227-01-24	FortiManager Cloud Device Based Subscription Service x Year Subscription for 100 devices/vdoms managed by FortiManager Cloud. FortiCare Premium Support is included.	2	Licencia	24 Meses

FORTIGATE 400F

El firewall de nueva generación (NGFW) FortiGate serie 400F combina seguridad basada en inteligencia artificial (IA) y aprendizaje automático (ML) para ofrecer protección frente a amenazas a cualquier escala. Obtenga una visibilidad más profunda de su red y vea las aplicaciones, usuarios y dispositivos antes de que se conviertan en amenazas. Impulsada por la tecnología ASIC de Fortinet, la serie 400F ofrece capacidades de detección de amenazas líderes en el sector, lo que permite identificar y mitigar las ciber amenazas de forma más rápida. La serie FortiGate 400F, impulsada por un rico conjunto de capacidades de seguridad AI/ML que se extienden en una plataforma integrada Security Fabric, ofrece una red segura que es amplia, profunda y automatizada. Asegure su red de extremo a extremo con protección de borde avanzada que incluye seguridad web, de contenido y de dispositivos, mientras que la segmentación de red y SD-WAN segura reducen la complejidad y el riesgo en redes de TI híbridas. El acceso universal a la red de confianza cero (ZTNA) controla, verifica y facilita automáticamente el acceso de los usuarios a las aplicaciones, reduciendo las amenazas laterales al proporcionar acceso solo a usuarios validados. La protección ultrarrápida frente a amenazas y la inspección SSL proporcionan seguridad en el borde visible sin afectar al rendimiento.

1 Módulo de plataforma de confianza (TPM)
La serie FortiGate 400F incluye un módulo dedicado que protege los dispositivos físicos de red generando, almacenando y autenticando claves criptográficas basado en hardware los mecanismos que protegen contra software malicioso y ataques de phishing.

2 Doble fuente de alimentación
La redundancia de la fuente de alimentación es fundamental para el funcionamiento de las redes de misión crítica. La serie FortiGate 400F cuenta con dos fuentes de alimentación integradas no intercambiables en caliente.

3 Seguridad en la capa de acceso
El protocolo FortiLink le permite converger la seguridad y el acceso a [illegible] ante la integración del FortiSwitch en el FortiGate como una extensión lógica del cortafuegos. Estos puertos [illegible] para FortiLink pueden reconfigurarse como puertos normales según sea necesario.
4 Conmutador Hardware de Firmware Firmado

El Conmutador de Firmware Firmado es un conmutador de seguridad físico. Por defecto, está configurado al nivel de nivel de seguridad. El nivel de seguridad más alto asegura que sólo un firmware FortiOS correctamente validado en el FortiGate. Esta característica añade una capa física extra de FortiGate que actúa como un importante elemento disuasorio y reduce el riesgo de compromiso.

FORTIGATE 120G

El cortafuegos de nueva generación (NGFW) FortiGate serie 120G combina seguridad basada en inteligencia artificial (IA) y aprendizaje automático (ML) para ofrecer protección frente a amenazas a cualquier escala. Obtenga una visibilidad más profunda de su red y vea las aplicaciones, usuarios y dispositivos antes de que se conviertan en amenazas. Impulsada por la tecnología ASIC de Fortinet, la serie 120G ofrece capacidades de detección de amenazas líderes en el sector, lo que permite identificar y mitigar las ciber amenazas de forma más rápida. La serie FortiGate 120G, impulsada por un rico conjunto de capacidades de seguridad AI/ML que se extienden en una plataforma integrada Security Fabric, ofrece una red segura que es amplia, profunda y automatizada. Asegure su red de extremo a extremo con protección de borde avanzada que incluye seguridad web, de contenido y de dispositivos, mientras que la segmentación de red y SD-WAN segura reducen la complejidad y el riesgo en redes de TI híbridas. IPS Universal, Zero Trust Network Access (ZTNA) controla, verifica y facilita automáticamente el acceso de los usuarios a las aplicaciones, reduciendo las amenazas laterales al proporcionar acceso solo a usuarios validados. La protección ultrarrápida frente a amenazas y la inspección SSL proporcionan seguridad en el borde visible sin afectar al rendimiento.
1 Trusted Platform Module (TPM)

La serie FortiGate 120G incorpora un módulo dedicado que protege los dispositivos físicos de red mediante la generación, el almacenamiento y la autenticación de claves criptográficas. Los mecanismos de seguridad basados en hardware protegen contra el malware y los ataques de phishing.
2 Doble fuente de alimentación

La redundancia de la fuente de alimentación es esencial en el funcionamiento de redes de misión crítica. La serie FortiGate 120G ofrece fuentes de alimentación duales integradas no intercambiables en caliente.
3 Seguridad de la capa de acceso

El protocolo FortiLink permite converger la seguridad y el acceso a la red integrando el FortiSwitch en el FortiGate como una extensión lógica delcortafuegos. Estos puertos habilitados para FortiLink pueden reconfigurarse como puertos normales según sea necesario.

FORTIGATE 600F

El cortafuegos de nueva generación (NGFW) FortiGate serie 600F combina seguridad basada en inteligencia artificial (IA) y aprendizaje automático (ML) para ofrecer protección frente a amenazas a cualquier escala. Obtenga una visibilidad más profunda de su red y vea las aplicaciones, usuarios y dispositivos antes de que se conviertan en amenazas. Impulsada por la tecnología ASIC de Fortinet, la serie 600F ofrece capacidades de detección de amenazas líderes en el sector, lo que permite identificar y mitigar las ciber amenazas de forma más rápida. La serie FortiGate 600F, impulsada por un rico conjunto de capacidades de seguridad AI/ML que se extienden en una plataforma integrada Security Fabric, ofrece una red segura que es amplia, profunda y automatizada. Asegure su red de extremo a extremo con protección de borde avanzada que incluye seguridad web, de contenido y de dispositivos, mientras que la segmentación de red y SD-WAN segura reducen la complejidad y el riesgo en redes de TI híbridas. IPS Universal, Zero Trust Network Access (ZTNA) controla, verifica y facilita automáticamente el acceso de los usuarios a las aplicaciones, reduciendo las amenazas laterales al proporcionar acceso solo a usuarios validados. La protección ultrarrápida frente a amenazas y la inspección SSL proporcionan seguridad en el borde visible sin afectar al rendimiento.

1 Trusted Platform Module (TPM)

La serie FortiGate 600F incorpora un módulo dedicado que protege los dispositivos físicos de red mediante la generación, el almacenamiento y la autenticación de claves criptográficas. Los mecanismos de seguridad basados en hardware protegen contra el malware y los ataques de phishing.
2 Doble Fuente de alimentación

La redundancia de la fuente de alimentación es esencial en el funcionamiento de redes de misión crítica. La serie FortiGate 600F ofrece fuentes de alimentación duales integradas no intercambiables en caliente.

3 Seguridad de la capa de acceso

El protocolo FortiLink permite converger la seguridad y el acceso a la red integrando el FortiSwitch en el FortiGate como una extensión lógica del cortafuegos. Estos puertos habilitados para FortiLink pueden reconfigurarse como puertos normales según sea necesario.

FUNCIONALIDADES FIREWALL FORTIGATE

La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión [illegible];

- Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;

- Las funcionalidades de protección de red que conforman la plataforma de seguridad pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;
- La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;
- Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación;
- La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;
- Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;
- Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;
- Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;
- Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);
- Los dispositivos de protección de red deben soportar DHCP Relay;
- Los dispositivos de protección de red deben soportar DHCP Server;
- Los dispositivos de protección de red deben soportar sFlow;
- Los dispositivos de protección de red deben soportar Jumbo Frames;
- Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;
- Debe ser compatible con NAT dinámica (varios-a-1);
- Debe ser compatible con NAT dinámica (muchos-a-muchos);
- Debe soportar NAT estática (1-a-1);
- Debe admitir NAT estática (muchos-a-muchos);
- Debe ser compatible con NAT estático bidireccional 1-a-1;
- Debe ser compatible con la traducción de puertos (PAT);
- Debe ser compatible con NAT Origen;
- Debe ser compatible con NAT de destino;
- Debe soportar NAT de origen y NAT de destino de forma simultánea;
- Debe soportar NAT de origen y NAT de destino en la misma política
- Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;
- Debe ser compatible con NAT64 y NAT46;
- De Debe soportar SD-WAN de forma nativa
- Debe soportar el balanceo de enlace hash por IP de origen;
- Debe soportar el balanceo de enlace por hash de IP de origen y destino;
- Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces;
- Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;
- Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;
- Enviar logs a sistemas de gestión externos simultáneamente;
- Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;
- Debe soporta protección contra la suplantación de identidad (anti-spoofing);
- Implementar la optimización del tráfico entre dos dispositivos;
- Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);
- Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);
- Soportar OSPF graceful restart;
- Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;
- Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;
- Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;
- Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;
- Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;
- Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;
- Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;
- La configuración de alta disponibilidad debe sincronizar: Sesiones;
- La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;
- La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;
- La configuración de alta disponibilidad debe sincronizar: Tablas FIB;
- En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
- Debe soportar la creación de sistemas virtuales en el mismo equipo;
- Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;
- Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;be implementar el protocolo ECMP.
- La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;
- Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente e[illegible]s virtuales (contextos);
- Debe soportar una malla de seguridad para proporcionar una s[illegible]seguridad integral que abarque toda la red;
- El tejido de seguridad debe identificar potenciales vulnerabilidad[illegible]r las mejores prácticas que podrían ser

usadas para mejorar la seguridad general y el rendimiento de una red;
- Debe existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW;
- La consola de administración debe soportar como mínimo, inglés, español y portugués.
- La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad
- La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.

FIREWALL

- Debe soportar controles de zona de seguridad;
- Debe contar con políticas de control por puerto y protocolo;
- Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;
- Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;
- Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;
- Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;
- Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.
- Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);
- Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes
- Debe soportar el protocolo estándar de la industria VXLAN;
- La solución debe permitir la implementación sin asistencia de SD-WAN
- En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN;
- La solución debe soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.

APP CONTROL

- Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;
- Detección de miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;
- Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
- Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor;
- Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;
- Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
- Actualización de la base de firmas de la aplicación de forma automática;
- Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos;
- Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
- Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;
- El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
- Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;
- Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
- Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Hangouts el chat, pero impedir la llamada de video;
- Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;
- Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de estas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc);
- Debe ser posible crear grupos dinámicos de aplicaciones basa[illegible]cterísticas de las mismas, tales como: Nivel de riesgo de la aplicación;

- Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;
- Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente

THREAT PREVENTION

- Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;
- Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);
- Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;
- Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;
- Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos;
- Deber permitir el bloqueo de vulnerabilidades y exploits conocidos
- Debe incluir la protección contra ataques de denegación de servicio;
- Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;
- Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;
- Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;
- Debe tener los siguientes mecanismos de inspección IPS: Reensamblado de paquetes TCP;
- Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);
- Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc;
- Detectar y bloquear los escaneos de puertos de origen;
- Bloquear ataques realizados por gusanos (worms) conocidos;
- Contar con firmas específicas para la mitigación de ataques DoS y DDoS;
- Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);
- Debe poder crear firmas personalizadas en la interfaz gráfica del producto;
- Identificar y bloquear la comunicación con redes de bots;
- Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo.
- Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
- Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;
- Los eventos deben identificar el país que origino la amenaza;
- Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
- Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;
- Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;
- En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles;
- Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube);

URL FILTER

- Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);
- Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito;
- Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;
- Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL;
- Tener por lo menos 75 categorías de URL;
- Debe tener la funcionalidad de exclusión de URLs por categoría;
- Permitir página de bloqueo personalizada;
- Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);
- Además del Explicit Web Proxy, soportar proxy web transparente
- 2.2.5.6 User Identity
- Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active

Directory, E-directorio y base de datos local;
- permitiendo granularidad a las políticas / controles basados en usuarios y grupos de usuarios;
- Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/controles basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;
- Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / controles basados en usuarios y grupos de usuarios;
- Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/controles basados en usuarios y grupos de usuarios;
- Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo);
- Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;
- Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;
- Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;
- Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;

QOS & SHAPING

- Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;
- Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;
- Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
- Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;
- En QoS debe permitir la definición de tráfico con ancho de banda garantizado;
- En QoS debe permitir la definición de tráfico con máximo ancho de banda;
- En QoS debe permitir la definición de colas de prioridad;
- Soportar marcación de paquetes DiffServ, incluso por aplicación;
- Soportar la modificación de los valores de DSCP para Diffserv
- Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);
- Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;

DLP

- Permite la creación de filtros para archivos y datos predefinidos;
- Los archivos deben ser identificados por tamaño y tipo;
- Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;
- Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;
- Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;
- Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares;

Geo IP

- Soportar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de cierto País/Países;
- Debe permitir la visualización de los países de origen y destino en los registros de acceso;
- Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;

VPN

• Soporte VPN de sitio-a-sitio y cliente-a-sitio;
• Soportar VPN IPSec;
• Soportar VPN SSL;
• La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512
• La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;
• La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);
• La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Adva[illegible]ption Standard);
• Debe tener interoperabilidad con los siguientes fabricantes: Cisco, [illegible], Juniper, Palo Alto Networks, Fortinet, SonicWall;
• Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de tú[illegible]PSec;

• Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting;
• Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy;
• Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL;
• Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;
Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;
• Deberá mantener una conexión segura con el portal durante la sesión;
• El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS

FORTISWITCH: FS-1024E, FS-148F, FS-124F-FPOE, FS-148F-FPOE

La familia de productos de acceso FortiSwitch™ está diseñada para satisfacer las demandas exclusivas de sucursales corporativas y pequeñas empresas. Una combinación incomparable de seguridad, facilidad de uso y escalabilidad hace que FortiSwitch™ sea la opción ideal para la infraestructura Ethernet.
Administrar una sucursal empresarial remota o una red de pequeñas empresas puede ser una tarea difícil debido a varios factores, entre ellos la falta de visibilidad de los dispositivos conectados, tiempo y herramientas limitados para la administración de LAN y la escasez de personal capacitado. La familia FortiSwitch Secure Access integra perfectamente la red Ethernet con funciones de seguridad avanzadas, eliminando de manera efectiva los silos que dificultan la administración diaria. FortiSwitch, rico en funciones y fácil de administrar con un bajo costo total de propiedad, surge como la opción óptima para redes Ethernet remotas de sucursales empresariales y pequeñas empresas.
Redes seguras a través de FortiLink
FortiLink es un innovador protocolo de gestión patentado que permite una integración y gestión perfectas entre un firewall de última generación FortiGate y la plataforma de conmutación Ethernet FortiSwitch. Al utilizar FortiLink, FortiSwitch se convierte en una extensión lógica de FortiGate, lo que permite la gestión centralizada de las funciones de seguridad de la red y de la capa de acceso a través de una única interfaz.
Control de acceso a la red (NAC) fácil de usar y sin costo
La integración de FortiLink permite la funcionalidad básica de NAC para perfilar e integrar de forma segura los dispositivos a medida que se conectan. FortiLink NAC ofrece visibilidad de todos los dispositivos conectados, segmentación automatizada y políticas de seguridad para dispositivos IoT, cuarentena en caso de riesgo y parches virtuales para ayudar a protegerse contra amenazas.

Seguridad del puerto Ethernet incorporado
La seguridad tradicional de los puertos Ethernet exige un esfuerzo manual y un mantenimiento continuo, lo que es poco práctico para los administradores de TI de sucursales remotas o pequeñas empresas. En consecuencia, los puertos Ethernet suelen quedar desprotegidos. La conmutación de acceso de FortiSwitch ofrece a los administradores de TI la capacidad de proteger los puertos y garantizar que solo los usuarios y dispositivos aprobados tengan acceso a la red. La automatización de la seguridad de los puertos sin necesidad de 802.1x hace que la aplicación de políticas sea fácil de implementar y administrar, mientras que las políticas de nivel NGFW garantizan un control granular y un acceso de confianza cero para usuarios y dispositivos.
Control de acceso y aplicación de políticas basados en usuarios y dispositivos
Ya sea que se utilice Fortinet Identity Access Management (IAM) o proveedores de identidad de terceros, la automatización de FortiLink puede aprovechar la identidad del usuario para tomar decisiones de políticas granulares basadas en roles, lo que le permite implementar principios de confianza cero.
Servicio de acceso seguro en el borde (SASE)
Esta arquitectura empresarial de FortiSwitch ofrece una base integrada para el acceso a la red de confianza cero (ZTNA) y el borde del servicio de acceso seguro (SASE), lo que ofrece la flexibilidad de implementar fácilmente el tipo y el nivel de seguridad que necesita en el borde de su red.
Campus central y centro de datos escalables y flexibles
La arquitectura empresarial de FortiSwitch se escala sin esfuerzo para satisfacer las demandas de los núcleos de campus y centros de datos de última generación de la actualidad, todo ello sin comprometer la seguridad. Al admitir hasta 48 puertos en un formato compacto de 1 RU, FortiSwitch minimiza el uso del espacio en rack al tiempo que ofrece el rendimiento y la escalabilidad necesarios. Cada serie de conmutadores de la familia de núcleos de campus y centros de datos ofrece modelos que permiten al administrador elegir el medio adecuado para su entorno a través de una amplia gama de transceptores Fortinet. Esta característica también se aplica a los enlaces ascendentes, con velocidades de hasta 100 GE que admiten varios medios.

FUNCIONALIDADES DE LOS FORTISWITCHES

- El switch deberá poder aceptar actualizaciones de firmware
- Los switches con PoE deberán tener la capacidad de habilitar o deshabilitar la función de PoE
- Deberá soportar detección y notificación de conflictos de direcciones IP
- Deberá soportar administración en la nube
- Deberá soportar administración por IPv4 e IPv6
- Deberá soportar Telnet / SSH para acceso a la consola
- Deberá soportar HTTP / HTTPS
- Deberá soportar SNMP v1/v2c/v3
- Deberá poder configurar su reloj mediante un NTP Server

- Deberá contar con una línea de comandos estándar y con interfaz para configurar vía Web
- Deberá soportar actualizaciones de Software por: TFTP/FTP/GUI
- Deberá soportar HTTP REST APIs para Configuración y monitoreo

ALTA DISPONIBILIDAD

- Deberá soportar Multi-Chassis LAG (MCLAG)
- Deberá soportar STP sobre Multi-Chassis LAG (MCLAG)

CALIDAD DE SERVICIOS

- Deberá soportar priorización de tráfico basada en 802.1p
- Deberá soportar priorización de tráfico basada en IP TOS/DSCP
- Deberá soportar marcado de tráfico con 802.1p y/o IP TOS/DSCP

LAYER 2

- Deberá soportar Link Aggregation estático
- Deberá soportar LACP
- Deberá soportar Spanning Tree
- Deberá soportar Jumbo Frames
- Deberá soportar Auto-negociacion para la velocidad de los puertos y para Duplex
- Deberá soportar el estandar IEEE 802.1D MAC Bridging/STP
- Deberá soportar el estandar IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
- Deberá soportar el estandar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
- Deberá soportar la funcionalidad STP Root Guard
- Deberá soportar STP BPDU Guard
- Deberá soportar Edge Port / Port Fast
- Deberá soportar el estándar IEEE 802.1Q VLAN Tagging
- Deberá soportar Private VLAN
- Deberá soportar el estándar IEEE 802.3ad Link Aggregation con LACP
- Deberá poder balancear tráfico Unicast/Multicast sobre un puerto trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac)
- Deberá soportar el estándar IEEE 802.1AX Link Aggregation
- Deberá soportar instancias de Spanning Tree (MSTP/CST)
- Deberá soportar el estándar IEEE 802.3x Flow Control con Back-pressure
- Deberá soportar el estándar IEEE 802.3 10Base-T
- Deberá soportar el estándar IEEE 802.3u 100Base-TX
- Deberá soportar el estándar IEEE 802.3z 1000Base-SX/LX
- Deberá soportar el estándar IEEE 802.3ab 1000Base-T
- Deberá soportar el estándar IEEE 802.3 CSMA/CD como método de acceso y las especificaciones de la capa física
- Deberá contar con la funcionalidad de Control de Tormentas (Storm Control)
- Deberá soportar la creación de VLANs por MAC, IP y Ethertype-based
- Deberá soportar la funcionalidad de Virtual-Wire
- Deberá soportar Time-Domain Reflectometer (TDR)
- Deberá soportar 4094 VLANs simultáneas
- Deberá soportar IGMP Snooping
- Deberá soportar IGMP proxy y querier
- Deberá soportar emergency location identifier numbers (ELINs) en LLDP-MED
- Deberá permitir la negociación de POE en LLDP-MED
- Deberá permitir limitar la cantidad de MACs aprendidas por puerto
- Deberá permitir un mínimo de 15 instancias de MSTP
- Deberá permitir controlar tormentas de broadcast independientemente en cada puerto
- Deberá soportar un mecanismo de detección y prevención de loops
- Deberá soportar VLAN Stacking (QinQ)
- Deberá soportar SPAN
- Deberá soportar RSPAN y ERSPAN

LAYER 3

- Deberá soportar ruteo estático
- Deberá soportar RIP v2
- Deberá soportar OSPF v2
- Deberá soportar VRRP
- Deberá soportar IS-IS
- Deberá soportar BGP
- Deberá soportar protocolos de ruteo multicast
- Deberá soportar Equal Cost Multipath Routing (ECMP)
- Deberá soportar Bidirectional Forwarding Detection (BFD)
- Deberá soportar DHCP Relay
- Deberá soportar DHCP Server

RFCS

- Deberá soportar el RFC 2571 Architecture for Describing SNMP
- Deberá soportar DHCP Client
- Deberá soportar el RFC 854 Telnet Server
- Deberá soportar el RFC 2865 RADIUS
- Deberá soportar el RFC 1643 Ethernet-like Interface MIB
- Deberá soportar el RFC 1213 MIB-II
- Deberá soportar el RFC 1354 IP Forwarding Table MIB
- Deberá soportar el RFC 2572 SNMP Message Processing and Dispatching
- Deberá soportar el RFC 1573 SNMP MIB II
- Deberá soportar el RFC 1157 SNMPv1/v2c
- Deberá soportar el RFC 2030 SNTP

SECURITY & VISIBILITY

- Deberá soportar Port Mirroring
- Deberá soportar Admin Authentication Via RFC 2865 RADIUS
- Deberá soportar el estándar IEEE 802.1x authentication Port-based
- Deberá soportar el estándar IEEE 802.1x Authentication MAC-based
- Deberá soportar el estándar IEEE 802.1x Guest and Fallback VLAN
- Deberá soportar el estándar IEEE 802.1x MAC Access Bypass (MAB)
- Deberá soportar el estándar IEEE 802.1x Dynamic VLAN Assignment
- Deberá soportar Radius CoA (Change of Authority)
- Deberá soportar el estándar IEEE 802.1ab Link Layer Discovery Protocol (LLDP)
- Deberá soportar el estándar IEEE 802.1ab LLDP-MED
- Deberá soportar Radius Accounting
- Deberá soportar EAP pass-through
- Deberá soportar detección de dispositivos
- Deberá soportar MAC-IP binding
- Deberá soportar sFlow
- Deberá soportar Flow Export
- Deberá soportar ACLs
- Deberá soportar múltiples ACLs de ingreso
- Deberá soportar scheduling de ACLs
- Deberá soportar DHCP Snooping
- Deberá soportar listas de servidores DHCP permitidos
- Deberá soportar bloqueo de DHCP
- Deberá permitir Dynamic ARP Inspection (DAI)
- Deberá permitir Access VLANs
- Deberá permitir tagging de tráfico con VLAN ID mediante ACLs

OTHER

- Deberá soportar Syslog
- Debe contar con un sensor de temperatura interno
- Debe permitir monitorear la temperatura del dispositivo
- Debe soportar QSFP+ low-power mode
- Debe soportar Energy-Efficient Ethernet (EEE)
- Debe soportar QSFP+ low-power mode
- Debe soportar Energy-Efficient Ethernet (EEE)

FAP-231G-N

Los puntos de acceso FortiAP™ se administran de manera centralizada mediante el controlador WLAN integrado de cualquier dispositivo de seguridad FortiGate® o mediante el portal de administración y aprovisionamiento de FortiEdge Cloud. Con la integración de la funcionalidad del controlador inalámbrico en el dispositivo FortiGate líder del mercado, estos puntos de acceso son perfectos para implementaciones en campus y sucursales. Security Fabric de Fortinet le permite administrar fácilmente la seguridad cableada e inalámbrica desde una consola de administración de panel único y protege su red de las últimas amenazas de seguridad. Aspectos destacados

- La consola de administración unificada simplifica las operaciones, lo que garantiza la coherencia en la aplicación y el cumplimiento de políticas efectivas
- Base integrada para el acceso a la red de confianza cero (ZTNA) y el servicio de acceso seguro en el borde (SASE), lo que le permite la flexibilidad de implementar fácilmente microsucursales con la seguridad que necesita en el borde de su red
- Seguridad de LAN inalámbrica bien hecha, del líder en seguridad de redes. Firewall integrado, IPS, control de aplicaciones y filtro web protegen la LAN inalámbrica de las amenazas de seguridad más recientes
- Protege la red de amenazas inalámbricas avanzadas y cumple con los requisitos de la industria, como PCI DSS.

FORTIANALYZER 300G

FortiAnalyzer es una potente plataforma de gestión de registros, análisis y [illegible] que proporciona a las organizaciones una única consola para gestionar, automatizar, orquestar y respo[illegible]e permite operaciones de seguridad simplificadas, identificación y remediación proactiva de riesgos y visi[illegible]oleta de todo el panorama de ataques.

Integrado con Fortinet Security Fabric, FortiAnalyzer brinda a los equipos de operaciones de seguridad y redes capacidades de detección en tiempo real, análisis de seguridad centralizado y conocimiento de la postura de seguridad de extremo a extremo para ayudar a los analistas a identificar amenazas persistentes avanzadas (APT) y mitigar los riesgos antes de que pueda ocurrir una infracción.

- Monitoreo y visibilidad de red centralizados
- Detección avanzada de amenazas y vulnerabilidades con correlación de datos de eventos y registros
- Operaciones de NOC/SOC aumentadas para respuesta, análisis e informes en tiempo real
- Automatización para ahorrar tiempo, reducir errores y mejorar la eficiencia
- Solución multiusuario con administración de cuotas
- Dominios administrativos para efectividad operativa y cumplimiento
- Más de 70 informes y más de 2000 conjuntos de datos, gráficos y macros listos para usar

Activos e identidad

FortiAnalyzer Fabric View con monitoreo de activos e identidad brinda a los equipos de SOC mayor conocimiento y visibilidad de los puntos finales y usuarios de una organización con paneles de control e información correlacionada de dispositivos y UEBA, detecciones de vulnerabilidades, etiquetado de EMS y clasificaciones de activos a través de telemetría con EMS, NAC, Fortinet Fabric Agent y una vista de panel de OT.

FORTINET TRANSCEIVERS / CABLE (FN-CABLE-SFP+5)

Los problemas de conectividad habituales en las redes de empresas y centros de datos suelen deberse a módulos transceptores incompatibles y de baja calidad, más que a un fallo en los propios dispositivos de red. Los transceptores de Fortinet han sido especialmente diseñados y probados para funcionar con equipos Fortinet, garantizando que su red sea lo más estable y robusta posible, y eliminando las conjeturas a la hora de seleccionar transceptores compatibles. Amplia gama para una máxima flexibilidad Los transceptores Fortinet, compatibles con varios factores de forma, tipos de medios y rendimiento, proporcionan opciones de conectividad para satisfacer muchas arquitecturas de red y escenarios de despliegue diferentes. Tanto si su red requiere 400 GE de alta velocidad dentro del centro de datos, como 1 GE de largo alcance para conectar centros de datos en diferentes ciudades, Fortinet tiene un transceptor para satisfacer sus necesidades.

FORTINET - POE INJECTOR (GPI-130)

CUMPLIMIENTO CONDICIONES TECNICAS

La empresa debe cumplir con lo solicitado en el presente anexo técnico
La empresa aprovisionara, instalará, implementara y realizar el soporte de los equipos ofertados y requeridos en las bases técnicas.
Se realizará la implementación solicitada en las presentes condiciones técnicas, de existir una mejora se notificará a INDAP para su validación y aprobación en caso de ser implementado.

FIREWALL

- Se debe implementar **2x FG-600F** en **HA** para la sucursal, DATA CENTER
- Se debe implementar **2xFG-400F** en **HA** para la sucursal, NIVEL CENTRAL
- Se debe implementar **16xFG-120G** para las sucursales restante (Direcciones regionales, oficinas de area, oficinas de apoyo).

EQUIPO DE MONITOREO Y REPORTES

- Se debe implementar **1XFAZ-300G** para la sucursal de, DATA CENTER.

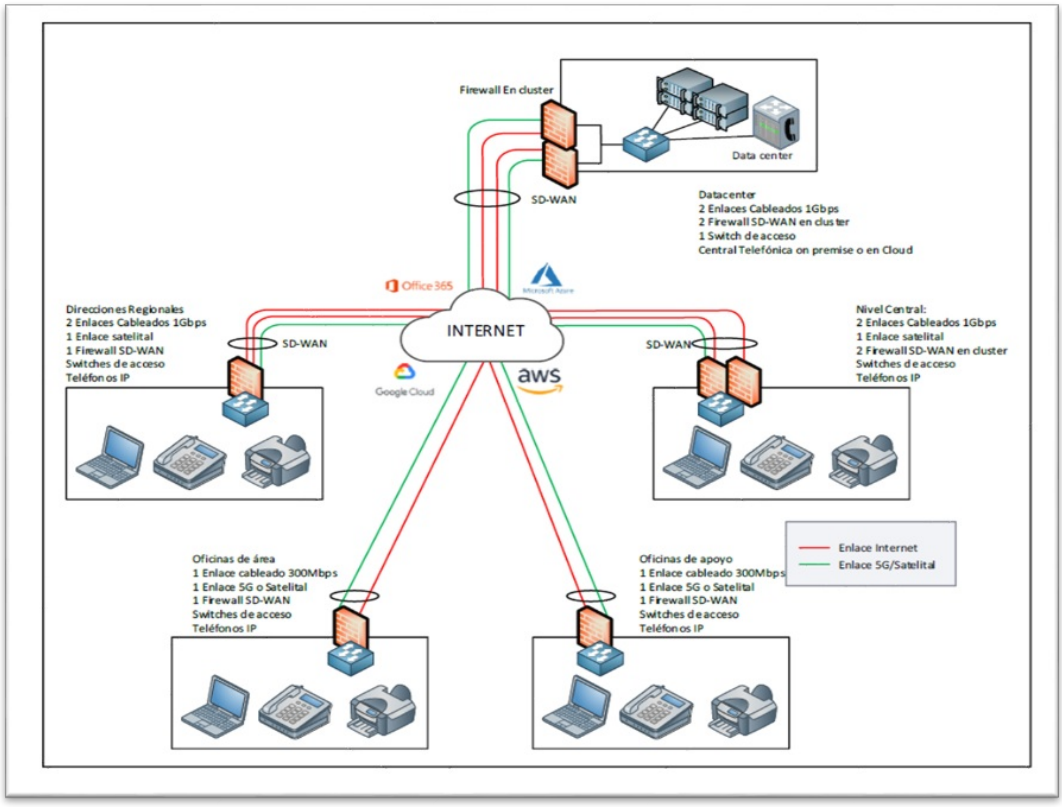
ACCESS POINT

- Se debe implementar **43XFAP-231G-N** distribuidos en las sucursales restantes.

IMPLEMENTACION

- Para la implementación SD-WAN y los AP con el equipamientiento de Fortinet ofertado, consideraran la configuración del HA de los firewall en 2 Sucursales, con implementación de VDom y configuración de políticas básicas como también mejoras de estas, por parte del proveedor y INDAP. Por último se harán pruebas del servicio para saber si esta todo correcto.
- Se deben enviar las certificaciones del personal que estará a cargo del proceso de implementación y soporte durante el contrato, asegurando en todo momento que solo personal certificado será responsable de entregar el servicio. Si durante el contrato parte del personal cambia se deberá informar y enviar los antecedes del nuevo personal.
- En el caso de los Switch, se considera la Configuración del HA en 2 de las sedes y conectividad con los **2XFG-600F Y 2XFG-400F**, para la implantacion de los HA y de la red SD-WAN.
- Se considera la configuración de los **16XFG-120G** dentro de la red SD-WAN para todas las demás sucursales excluyendo **DATA CENTER y NIVEL CENTRAL**
- En el caso con los Access Point, **43XFAP-231G**, se considerará la configuración de conectividad y bandas con las mejores buenas practicas.
- Con la finalidad de optimizar el tiempo de configuración, se requiere que equipamiento Fortinet estén disponibles en INDAP con 2 semanas de antelación al inicio de trabajos, con la configuración básica precargada.
- Entregar carta Gantt con plazos claramente estipulados y puntos de Rollback en caso de inconvenientes.
- La empresa asume los viáticos, estadía y compensaciones por posibles trabajos fuera de horario laboral o en fin de semana del personal que habilitará los servicios en terreno, en un 100%.
- La totalidad de los equipos, son completamente nuevos y sin uso. En caso de que algún equipo sea usado, se rechazará, lo que conllevara la aplicación de multas por el retraso en la llegada e instalación de equipos.
- Para optimizar los tiempos de configuración, requiere anticipadamente (una vez suscrito iniciados los servicios) los accesos a los equipos FW actuales y SW (user y password mas la Ip), y la VPN si en caso que sea necesario para las pruebas de servicio.

DIAGRAMA SD-WAN DE FORTINET DE INDAP



DESPACHO

Todo el equipamiento antes señalado sera trasladado y entregado en las dependencias del Cliente, según corresponda. En caso de retraso en la llegada de los productos a INDAP de cualquier índole, esto debe sera resuelto por el prestador y en ningún caso traspasar la responsabilidad a INDAP, es obligación de la empresa anticipar retrasos y otras problemáticas de logística.

INSTALACION Y CONFIGURACION DE LOS NUEVOS EQUIPOS FO[illegible]00F, 400F Y 120G.

Se incluyen mínimo las siguientes actividades:

- Reunion Inicial -Kickoff
- Instalación de los nuevos equipos
- Levantamiento de informacion de la plataforma actual para la planificacion de actividades
- Configuracion inicial, considerando la instalación de las últimas versiones de sistema operativo y/o firmware para todos los modulos de seguridad de los nuevos firewalls. Los firewalls deberán quedar con las últimas actualizaciones de versiones del SO y firmware estables, y todos los modulos actualizados.
- Replicar la configuración de los equipos Fortigate (equipos nuevos) de manera de crear las zonas de seguridad, que se asociaran con las distintas interfaces de los actuales firewall, las zonas para considerar deberían ser al menos WAN, LAN DMZ, WIFI, WAF y cualquier otra que pudiese ser requeridos de acuerdo con las mejores prácticas.
- La migración (si en caso que se requiera) se realizara mediante la creación de VDOM en el nuevo equipo Fortigate.
- Los nuevos firewalls podrán ser configurados en modo offline de manera de prepararlos para la fecha de puesta en producción, la cual será coordinado con la institución.
- Todos firewalls serán configurados en HA según lo requerido, la cual será probada al momento de la puesta en producción. Cualquier inconveniente será será revisado por el ingeniero a cargo.
- La puesta en producción será realiza fuera de horario hábil, previa coordinación con la institución.
- Se configurarán todos los modulos disponibles bajo la licencia Fortinet UTP.
- Se implementarán configuraciones adicionales que permitan dejar los firewalls con los más altos estándares de seguridad.
- Se entregará la documentación respecto a la implementacion realizada y configuraciones realizadas.
- Se entregará un diagrama de conexión final, entre el firewall y los equipos conectados con la identificación de interfaces.
- Configuración de respaldo de configuraciones en Servidor de Backup.

Al finalizar la etapa de implementación se incluye:

- Memoria técnica de la plataforma implementada
- Evidencia de cumplimento de lo solicitado en las bases técnicas
- Informe final de proyecto
- Transferencia de conocimiento de la plataforma implementada para todo el personal que requiera la INDAP.

INSTALACION Y CONFIGURACION FORTIANALIZER

Se incluye el servicio de implementación de 1 FortiAnalyzer, versión física.

- Instalación de los equipos en el espacio indicado
- Registro de dispositivos para recolección y análisis de logs
- Pruebas y validaciones
- Se entregará la documentación respecto a la implementacion realizada y configuraciones realizadas.
- Se entregará un diagrama de conexión final, entre los dispositivosy los equipos conectados con la identificación de interfaces.
- Configuración de respaldo de configuraciones en Servidor de Backup

INSTALACION Y CONFIGURACION FORTIAP

Se incluye el servicio de implementación de 43 FortiAP distribuidos por las sucursales.

- Instalacion de los equipos en el espacio indicado
- Configuracion parametros de red, conectividad y bandas.
- Pruebas y validaciones
- Se entregara la documentación respecto a la implementacion realizada y configuraciones realizadas.
- Se entregara un diagrama de conexión final, entre los dispositivosy los equipos conectados con la identificación de interfaces.
- Configuracion de respaldo de configuraciones en Servidor de Backup

INSTALACION, Y CONFIGURACION FORTISWITCH.

EL servicio incluye la instalación y configuración de los equipos Fortiswitch ofertados.

- Levantamiento de información de la infraestructura actual
- Diseño de plan de trabajo de migración.
- Creación de vlan, ACL, interfaces, LACP, PAGP, control de acceso, y todo lo necesario para la correcta migración.
- Integración de los equipos con los Fortigate, Fortianalizer y Fortimanager.
- Pruebas y validaciones.
- Documentación de la implementación realizada.
- Diagrama final de conexión de los dispositivios.
- Configuración de respaldo de configuraciones en Servidor de Ba

2.-SERVICIO DE DATACENTER

En conformidad a los requerimientos técnicos definidos para el servicio de Datacenter se debe proporcionar un espacio seguro y optimizado para alojar servidores y equipos de hardware más los equipos INDAP actualmente en operación en DC Equinix ST1 (Ex DC CDLV Entel)
Se de contar con al menos DC Equinix ST1 el que actualmente cuenta con clasificación TIER III y que considera lo siguiente:
Espacio en Rack: Cuatro (4) racks de 42UR y 4kVA cada uno, proporcionando suficiente capacidad de energía para equipos de comunicaciones, servidores y equipos adicionales.
Energía: Sistemas de alimentación ininterrumpida (UPS) y grupos electrógenos para asegurar un suministro eléctrico continuo y sin interrupciones.
Conexiones: Se considera reflejos y patch panel entre rack.
Climatización: Sistemas avanzados de climatización, para mantener una temperatura óptima y evitar el sobrecalentamiento de los equipos.
Seguridad: Medidas de seguridad física y digital, incluyendo vigilancia 24/7, control de acceso y protección contra amenazas externas no autorizadas.
Soporte Técnico: Soporte técnico 24/7 para resolver cualquier problema técnico rápidamente.

- Monitoreo y Gestión: Monitoreo continuo de la conectividad, energía y otros parámetros críticos, con alertas automáticas en caso de problemas.
- Acceso: Acceso físico a los racks para mantenimiento y reparaciones.
- Este tipo de servicio es ideal para empresas que necesitan un entorno de alojamiento seguro y eficiente para sus servidores y equipos críticos.

Traslado Interno

Se debe efectuar el traslado (mudanza) de los equipos INDAP actualmente en operación dentro del mismo Datacenter Equinix TIER IV y que son de propiedad del actual proveedor de INDAP, ENTEL a la nueva ubicación ST1, pero TIER III.
Para todos los efectos de dimensionamiento y estimación de trabajos, se asume que los 4 rack considerados se utilizarán al 80 % quedando capacidad de alojamiento de futuros equipos.
La infraestructura considerada para esta estimación incluye el equipamiento contenido en los 4 racks completamente equipados que INDAP tiene actualmente operativos.
El traslado de equipos a sus nuevas ubicaciones debe ser realizado por la empresa con un equipo de trabajo especializado para cada una de las fases de la logística de transporte, con experiencia en el rubro, reduciendo de esta forma los riesgos asociados a la manipulación de herramientas, equipos, ingreso y circulación en la sala, y el transporte mismo de los equipos.

IV.-PLAZO IMPLEMENTACIÓN.
Para la ejecución del proyecto se estima un plazo de 90 días hábiles, contados a partir de la fecha de suscripción del contrato de servicios finalizando el 2 de octubre de 2025.
V.- DESARROLLO DE LO REQUERIDO.
Para el desarrollo de la solución requerida se debe tener presente lo siguiente:
VI.- SERVICIO DE SOPORTE Y POST VENTA.
Servicios que deben ser incluidos en soporte:
Se debe incluir el soporte y servicio post-venta durante la vigencia del contrato, con la finalidad de mantener la continuidad operativa de la plataforma implementada.
En caso de fallas ya sea de servicio como de equipamiento, se debe entregar una mesa de ayuda donde nos puedan dar, asistencia respectiva, en el menor tiempo posible.

- El contacto debe ser tanto vía telefónica como por correo.
- Tener la opción de seguimiento de casos mediante sistema de Ticket, Nro. de caso o similar.

- Fallas de la plataforma, como mínimo, deben estar cubiertos las siguientes:
- Fallas que impliquen caída total o parcial del sistema
- Incomunicación masiva
- En caso de fallas, se oferta SLA de respuesta de **15 min hábiles** y de resolución de problema en máximo 4 horas hábiles
- Configuraciones avanzadas
-

La empresa debe contar con personal especialista en el equipamiento instalado.
Se debe considerar soporte mensual por un especialista certificado en la marca, con al menos certificación **NSE 7** o superior.

Estas horas podrán ser utilizadas para:
Prioridad 1

- Actualizaciones de Firmware
- Aplicaciones de parches de seguridad
- Ingreso de Hash de seguridad

Prioridad 2

- Implementaciones de nuevas reglas
- Optimización de Reglas
- Optimización de Rutas
- Las actividades indicadas como Prioridad 1 tendrán como como máximo de ejecución **24 horas.**
- Las actividades indicadas como Prioridad 2 tendrán como como máximo de ejecución **48 horas.**

La empresa de forma mensual entregará un informe del estado del servicio con al menos los siguientes hitos:

- Cantidad de tickets/Casos atendidos.
- Actividades proactivas realizadas.
- Recomendaciones y conclusiones.

La empresa debe considerar de forma mensual una reunión de seguimiento post-implementacion del proyecto, para revisión del informe mensual y trabajos proactivos a realizar para el máximo aprovechamiento de la infraestructura implementada.
Se debe contar con un procedimiento de escalamiento, tanto técnico como comercial, con la finalidad de poder contactar a niveles superiores en caso de no contar con la satisfacción del servicio entregado.

MESA DE AYUDA

La empresa debe incluir en su Mesa de ayuda tiempos 24x7 para la creación de tickets para requerimientos y/o incidencias, mediante vía web, telefónica y/o correo electrónico.
Seguimiento de casos creados, para auditorías internas y registro de actividades.

- Desde el inicio de los servicios se debe dar acceso a la mesa de ayuda, así como manual del usuario y capacitación de la utilización
- Se puede hacer apertura casos vía telefónica, vía web y correo electrónico.

VII.- TIEMPOS DE RESPUESTAS Y SLA:

Los incidentes reportados se calificarán en las siguientes categorías, según el tipo de contexto del incidente:

Nivel de prioridad	Descripción	SLA Atención-Respuesta
Urgente	En estos incidentes no se pueden ejecutar ninguna de las funcionalidades y los usuarios no pueden trabajar.	15 Min
Alta	En estos incidentes no se pueden ejecutar algunas de las funcionalidades del producto, pero no esenciales para la operación del proceso.	1 hora
Media	Cliente o usuario en específico no puede operar o ejecutar alguna de las funcionalidades	2 horas
Baja	Cliente o usuario en específico envía una consulta respecto a configuraciones o características de los productos.	8 horas

Cobertura del servicio: De lunes a viernes de 09:00 a 18:00 horas se considera como horario hábil, y horario extendido (fuera de horario hábil)
El SLA de atención indica el tiempo máximo que el prestador compromete para darse por notificado de la incidencia y comenzar su diagnóstico y posterior resolución (si aplica) del problema reportado.
El SLA de resolución es variable y dependerá del problema reportado. En todo caso, el prestador siempre hará el mejor esfuerzo por resolverlo a la brevedad y con la posibilidad de ofrecer alternativas temporales que permitan reestablecer la funcionalidad perdida en menos de 4 Horas.
El incumplimiento en tiempos señalados será sancionado con 15 UF por cada hora de retraso en cada infracción verificada para los casos baja, media y alta y de 15 UF por cada 30 minutos de retraso en la categorización urgente.
Los niveles de servicio se refieren a la disponibilidad de éstos, donde se considera el total de minutos u horas sin servicio respecto del total de minutos u horas según corresponda, que contiene el mes evaluar.
VIII.-GARANTÍA DE EQUIPOS.
Se deberá garantizar los equipos durante la vigencia del contrato, de manera de asegurar la continuidad operativa del servicio.

IX.-TIEMPO DE ENTREGA DE EQUIPOS

El tiempo de entrega de los equipos será de 20 días a partir de la orde y/o suscripción del contrato.

X.-CONDICIONES DE INSTALACION.
INDAP proporcionará el espacio y energía necesario para alojar los equipos terminales

9.- Déjese establecido que la la personería del representante del prestador consta en escritura pública de Modificación de Sociedad de fecha 14 de marzo de 2025 suscrita ante don Christian Alejandro Ortíz Cáceres, Notario Público interino de la Séptima Notaría de Santiago, y anotada bajo el repertorio N°2.305-2025.

10.- Publíquese el presente acto administrativo, en el Sistema de Compras y Contratación Pública, Sitio www.mercadopublico.cl.

TOMESE RAZON, REGISTRESE Y TRANSCRIBASE,

ESTE DOCUMENTO CUENTA CON FIRMA ELECTRÓNICA AVANZADA
INDAP
Instituto de Desarrollo Agropecuario

MARIA ALEJANDRA SANCHEZ CORNEJO
Director Nacional (S)
Instituto De Desarrollo Agropecuario

Anexos

Nombre	Tipo	Archivo	Copias	Hojas
Certificado CBR	**Digital**	**Ver**		
Modificación sociedad	**Digital**	**Ver**		
Ficha Chileproveedores	**Digital**	**Ver**		
Garantia	**Digital**	**Ver**		
Informe tecnico y economico	**Digital**	**Ver**		
Informe art. 80	**Digital**	**Ver**		
PPT oferta indap	**Digital**	**Ver**		
contrato	**Digital**	**Ver**		
declaracion jurada	**Digital**	**Ver**		

MSC

Distribución:

DIVISIÓN FISCALIA

Documento firmado con Firma Electrónica Avanzada, el documento original disponible en:
https://ceropapel.indap.cl/validar/?key=39411039&hash=7beb3

CONTRALORIA GENERAL DE LA REPUBLICA CHILE 26-III-1927

TOMADO DE RAZÓN CON ALCANCES
Oficio: E108489/2025
POR ORDEN DE LA CONTRALORA GENERAL DE LA REPÚBLICA
Fecha: 30/06/2025
VICTOR HUGO MERINO ROJAS
Subcontralor General