

Términos y condiciones de contratación

I. Hiperenlace (Acceso a Internet de Banda Ancha).

Consiste en la provisión de conectividad dedicada y redundante mediante el uso de redes de fibra óptica y microondas de terceros concesionarios.

Incluye monitoreo proactivo y soporte de gestión operativa para minimizar latencias y optimizar el tráfico.

TÉRMINOS Y CONDICIONES APLICABLES:

1. El Suscriptor es totalmente responsable del uso que hagan sus usuarios finales del Servicio. Asimismo, el Suscriptor se compromete en cumplir y hacer que los usuarios finales cumplan con las leyes, regulaciones e instrucciones de uso aplicables al Servicio y se obliga a no se utilicen para fines ilegales. El incumplimiento de estas disposiciones podrá dar por resultado la remoción de las comunicaciones violatorias y/o la rescisión del presente contrato. Las interrupciones incluyen, de manera enunciativa pero no limitativa: 1) La distribución de publicidad no solicitada, 2) Correos electrónicos masivos o en serie (spam), 3) Propagación de virus informáticos, 4) Utilización de la red para realizar el ingreso no autorizado a cualquier otra máquina o equipo accesible a través de la red y cualquier consecuencia relacionada con ello. En caso de que alguna red u organismo bloquee las direcciones IP del Suscriptor por las razones anteriores, será obligación del Suscriptor gestionar el desbloqueo correspondiente.
2. El punto de demarcación entre la red de CIISTEC y la del Suscriptor será el Equipo CPE que se describe en la Propuesta Técnica.
3. Es responsabilidad del Suscriptor contar con el software adecuado en cada una de sus computadoras y realizar los cambios que sean necesarios en la configuración de su red, incluyendo el redireccionamiento de las direcciones IP asignadas a sus computadoras, de manera que permita que CIISTEC preste el Servicio. Es responsabilidad del Suscriptor la configuración, mantenimiento y correcto funcionamiento de sus equipos. El Suscriptor designará y mantendrá un representante técnico, quién será el responsable por parte del Suscriptor de la observancia y cumplimiento de los aspectos técnicos de este Anexo. En caso de que el SUSCRIPTOR decida nombrar a una persona diferente deberá dar aviso por escrito a CIISTEC y designar un nuevo responsable quien estará facultado para reportar a CIISTEC cualquier inconformidad o falla del Servicio.
4. Será obligación del Suscriptor, dentro de los 5 días hábiles siguientes a la firma del contrato entregar debidamente requisitado el formato de direcciones IP que le será entregado previamente por CIISTEC. En caso de que el Suscriptor no entregue el formato, o este no contenga toda la información solicitada, CIISTEC no será responsable de los problemas que se deriven por la falta de dicha información. El Suscriptor asume toda responsabilidad por la información que publique, envíe o reciba a través de Internet.

5. Las Partes acuerdan que el Servicio contratado es para uso exclusivo del Suscriptor y bajo ninguna circunstancia el Servicio podrá ser revendido o aprovechado por terceros bajo cualquier título legal, en caso de que el Suscriptor se encuentre en este supuesto, dará derecho a CIISTEC suspender el Servicio en forma inmediata y será considerado como causal de rescisión del presente contrato.
6. CIISTEC no será responsable de la configuración correspondiente a la interfaz del CPE proporcionado por el Suscriptor para la conexión a Internet.
7. El Suscriptor y sus usuarios finales, reconocen y aceptan que CIISTEC no opera y/o controla Internet y que todos los productos, información y servicios disponibles en el mismo, son ofrecidos por terceras partes, por lo que CIISTEC no tendrá responsabilidad de los mismos. El Suscriptor asume toda la responsabilidad y riesgo que derive del uso que le dé al servicio de acceso a Internet.
8. Bajo ninguna circunstancia CIISTEC será responsable de los daños y perjuicios que se deriven del mal uso o inhabilidad del Suscriptor para utilizar los servicios de CIISTEC o acceder a Internet o por la dependencia del usuario sobre la información, contenido o uso de la misma; por servicios o productos referidos localizados o adquiridos a través del servicio de CIISTEC; o por el resultado de errores, omisiones, interrupciones, pérdida alteración o robo de archivos, sistemas, aplicaciones, programas, procedimientos o información del Suscriptor por defectos o demora en la operación o transmisión o cualquier falla en el desempeño de Internet. CIISTEC no tendrá responsabilidad alguna por el mal uso, negligencia, uso fraudulento, contrario a especificaciones, ilegal y/o desautorizado que el Suscriptor haga del (los) Servicio(s).
9. ES responsabilidad del Suscriptor realizar el registro, pago y renovación de su dominio, al Register que este elija. A solicitud del Suscriptor CIISTEC podrá manejar dentro de sus DNSs los registros de hosts y/o solicitudes inversas de Direccionamiento IP (asignado por CIISTEC) previo pago que realice el Suscriptor.

II. Hiperconecta (Comunicaciones Unificadas / Telefonía en la Nube)

Servicio de telefonía basado en protocolos de internet (IP) y herramientas de colaboración híbrida.

Incluye, Integración nativa con sistemas CRM, movilidad total mediante aplicativos (softphones) y estandarización de flujos de atención. La responsabilidad de CIISTEC se limita a la configuración y gestión de la plataforma en la nube, no así a la conectividad de internet ajena a CIISTEC que el cliente utilice para acceder a ella.

TÉRMINOS Y CONDICIONES APLICABLES:

1. El saldo no utilizado en el periodo mensual no será reembolsable, ni acumulable para meses posteriores.
2. Para el mejor funcionamiento del servicio, CIISTEC asigna al Administrador del Servicio designado por el Suscriptor, contraseñas provisionales siendo obligación del Suscriptor cambiarlas en el primer uso que

haga de las mismas. Posterior al cambio de contraseñas El Suscriptor asume la responsabilidad sobre el uso de las contraseñas que establezca.

3. Para mayor seguridad y mejor control de llamadas de Larga Distancia Internacional en el Apéndice 2 de este Anexo, se detallan los destinos que quedan habilitados para cursar tráfico ("Lista Blanca"). Cualquier destino adicional que el Suscriptor requiera agregar a la Lista Blanca lo deberá solicitar por escrito a CIISTEC, en el entendido que aplica la tarifa Larga Distancia Resto del Mundo.
4. CIISTEC no maneja o provee garantías de Seguridad sobre su IP PBX, por lo tanto CIISTEC no asume ninguna responsabilidad por cualquier daño o perjuicio que pudiere sufrir el Suscriptor con motivo de cualquier ataque cibernético a su IP PBX.
5. El Suscriptor es exclusiva y totalmente responsable de establecer las medidas de seguridad que juzgue apropiadas para proteger su IP PBX de cualquier riesgo cibernético, y por lo tanto, el Suscriptor es totalmente responsable del pago del tráfico telefónico que se origine desde su IP PBX.
6. Los Servicios de Seguridad Administrada que provee CIISTEC excluyen expresamente la seguridad del IP PBX del Cliente.
7. El Suscriptor deberá contar previo a la prestación del Servicio, con un Equipo CPE (Customer Premises Equipment) que servirá como punto de demarcación entre la red de CIISTEC y la del Suscriptor.
8. Es responsabilidad del Suscriptor la configuración, mantenimiento y correcto funcionamiento de sus equipos. El Suscriptor designará y mantendrá un representante técnico, quién será el responsable por parte del Suscriptor de la observancia y cumplimiento de los aspectos técnicos de este Anexo. En caso de que el Suscriptor decida nombrar a una persona diferente deberá dar aviso por escrito a CIISTEC y designar un nuevo responsable quien estará facultado para reportar a CIISTEC cualquier inconformidad o falla del Servicio.
9. A fin de mitigar los riesgos por ataques a su IP PBX, CIISTEC pone a consideración del Suscriptor las siguientes recomendaciones de seguridad, en el entendido de que las mismas son meras recomendaciones generales que quedan al juicio del Suscriptor aplicarlas o no, y de ninguna manera CIISTEC asume responsabilidad de los ataques que el IP PBX del Suscriptor pudiere sufrir aún y cuando se apliquen dichas recomendaciones:
 - a) Es necesario que su IP PBX cuente con una política de contraseñas robustas para autenticar cada una de las extensiones de acuerdo con las especificaciones del fabricante del mismo.
 - b) Establecer estándares para identificar los teléfonos del PBX, por ejemplo RFC 4474, para evitar ataques de SPIT (SPAM for IP Telephony).

- c) Manejar esquemas de auto-configuración de teléfonos IP para evitar la manipulación del mismo archivo de configuración, y realizar las transferencias de archivos de configuración mediante el protocolo SFTP (Secure FTP).
 - d) Se recomienda no asignar una dirección IP homologada al PBX.
 - e) En caso de que el Suscriptor requiera tener un IP Homologada para dar acceso desde Internet a sus usuarios, se recomienda: Que los usuarios remotos tengan un acceso seguro al IP PBX mediante protocolos de encriptación como TLS para SIP y SRTP (Secure RTP), o bien IPSEC.
 - f) Realizar auditorías de seguridad a la red del IP PBX, incluyendo pruebas de penetración al menos dos veces al año.
 - g) Aplicar configuraciones de seguridad del IP PBX de acuerdo a recomendaciones del fabricante del mismo.
 - h) Establecer controles en el acceso a las funcionalidades del IP PBX como transferencia de llamadas, destinos de larga distancia, y celular.
 - i) Monitorear el comportamiento de los usuarios: número de llamadas, destinos, duración, para detectar comportamientos anormales del tráfico originado.
 - j) Implementar prácticas de Seguridad de la Información apegadas al estándar ISO 27001.
 - k) En los siguientes sitios donde puede consultar más recomendaciones de Seguridad para tecnologías basadas en VOIP: <http://www.uscert.org.au>; <http://www.cpni.gov.uk>; <http://www.us-cert.gov/cas/tips/ST05-018.html>; <http://www.cert.org/advisories/CA-2003-06.html>; <http://www.voipsa.org>.
10. Queda estrictamente prohibida la reventa, cesión o transferencia por cualquier forma del Servicio a cualquier tercero sin importar el propósito para el cual se lleve a cabo. El presente Contrato no confiere derecho para usar el Servicio TELEFONIA IP SIP para auto marcado ("Auto-Dialing"), uso continuo o excesivo de la funcionalidad de desvío de llamadas ("Call Forwarding"), Telemercadeo sin importar para que fin sea hecho ("Telemarketing"), el uso excesivo del servicio de fax ("Fax Broadcasting" o "Fax Blasting"). CIISTEC tiene el derecho de suspender el Servicio en forma inmediata si a su juicio el Suscriptor está usando el servicio para los fines antes mencionados o similares, así como a rescindir en forma inmediata el Contrato quedando el Suscriptor obligado a pagar las rentas mensuales del Servicio desde la fecha de rescisión hasta la fecha en la que concluya la vigencia del Contrato. Asimismo, CIISTEC notificará a las autoridades correspondientes con jurisdicción en caso de detectar este tipo de prácticas.
11. El Suscriptor podrá solicitar se le asigne nueva numeración para la prestación del servicio contratado o bien podrá utilizar la numeración con la que cuenta, en dicho supuesto se obliga a portar los números que tenga con su antiguo proveedor dentro de los 30 días siguientes a la fecha de Inicio del Servicio. CIISTEC

garantiza al Suscriptor una portabilidad efectiva, conforme a los términos y condiciones establecidos en las reglas de portabilidad vigentes.

III. Hiperalcance (Estrategia de Contacto Omnicanal – SMS, WhatsApp y RCS).

Servicios de mensajería masiva y comunicación interactiva para procesos de negocio y marketing.

Incluye la gestión de cuentas verificadas, diseño de flujos conversacionales mediante bots y análisis de tasas de apertura superiores al 90%. CIISTEC no es responsable por el contenido generado por el cliente ni por bloqueos impuestos por los dueños de las plataformas (Meta, Google o Carriers) derivados de malas prácticas de uso.

DESCRIPCIÓN Y ESPECIFICACIONES TÉCNICAS:

El Servicio consiste en el envío y/o recepción de Mensajes Cortos SMS conforme a los términos y condiciones establecidos en el presente anexo. El servicio se habilitará al Suscriptor mediante el establecimiento de una red privada virtual, mediante cualquier de las siguientes modalidades:

- Conexión SMS Gateway, en la cual CIISTEC pone a disposición del Suscriptor un portal web para el envío de los SMS.
- Conexión vía API, en el cual el Suscriptor conectará sus equipos directamente con la plataforma de Servicio de CIISTEC.

TÉRMINOS Y CONDICIONES APLICABLES:

1. El servicio únicamente incluye el envío y recepción de mensajes a números nacional.
2. Es responsabilidad del Suscriptor la configuración, mantenimiento y correcto funcionamiento de sus equipos. El Suscriptor designará y mantendrá un representante técnico, quién será el responsable por parte del Suscriptor de la observancia y cumplimiento de los aspectos técnicos de este Anexo. En caso de que el Suscriptor decida nombrar a una persona diferente deberá dar aviso por escrito a CIISTEC y designar un nuevo responsable quien estará facultado para reportar a CIISTEC cualquier inconformidad o falla del Servicio.
3. CIISTEC no será responsable por la no la entrega del SMS, en los siguientes supuestos:
 - a. El Equipo Terminal del usuario destino no tenga la funcionalidad de recibir SMS;

- b. El Usuario Destino: (i) tenga apagado su equipo terminal; (ii) tenga suspendido el servicio de SMS por cualquier causa; (iii) se encuentre fuera del área de cobertura de la red del operador móvil; o (iv) se encuentre en un área de cobertura exclusivamente analógica.
 - c. Cuando los mensajes enviados por el Suscriptor se ubiquen en los supuestos de Prácticas Prohibidas que se detallan a continuación.
4. Queda prohibido para el Suscriptor el envío de mensajes con las características siguientes, los cuales se consideran Prácticas Prohibidas:
- i. El envío de Spam:
Será considerado Spam el envío de 10 mensajes desde un mismo número en el transcurso de 1 (un) minuto.
 - ii. El envío de flooding: Será considerado como flooding, el envío de Mensajes Cortos con los siguientes parámetros:
 - El envío por parte de un mismo número de 10 (diez) Mensajes Cortos dirigidos al mismo destino en el transcurso de un minuto.
 - El envío por parte de un mismo número de más de 100 (cien) Mensajes Cortos en el transcurso de un minuto.
 - iii. Manipular, falsear o insertar información en alguno de los campos de los SMS intercambiados a través del protocolo SMPP.
 - iv. Realizar exploraciones en la arquitectura de cualesquiera de los elementos involucrados en el diagrama de conexión de la otra Parte, con el fin de buscar y/o explotar fallas en la seguridad.
 - v. Enviar cualquier tipo de mensaje que afecte la configuración/programación del Equipo Terminal del Usuario Destino.
 - vi. Enviar cualquier tipo de mensaje que pueda afectar, menoscabar o restringir la operación del equipo terminal del usuario destino (Código Malicioso).

IV. Hiperblindaje (Seguridad Perimetral Administrada)

Hiperblindaje es la gestión y resguardo de la integridad, confidencialidad y disponibilidad de la información del cliente. Implementación de barreras de seguridad perimetral administradas por ingenieros certificados de CIISTEC, CIISTEC garantiza la debida diligencia en la gestión, pero el cliente reconoce que no existe la seguridad informática absoluta frente a ataques de fuerza mayor o vulnerabilidades de software de terceros.

El servicio de HiperBlindaje provee protección a la red interna del Suscriptor estableciendo un punto de control entre ésta y su conexión a Internet mediante un equipo especializado en realizar funciones de

seguridad (en lo sucesivo, el “Firewall”) que se instala en sus oficinas.

Las políticas de seguridad son absoluta responsabilidad del Suscriptor.

La administración y mantenimiento del Firewall se realiza de manera centralizada desde CIISTEC. Cualquier cambio en la configuración de las políticas de seguridad debe ser expresamente solicitado por el Suscriptor vía correo electrónico y será realizado en coordinación con personal autorizado por el Suscriptor de acuerdo a la lista de personas que previamente envíe por escrito a CIISTEC, misma que deberá ser actualizada si existen cambios y notificada a CIISTEC con oportunidad.

Seguridad Administrada consiste en:

El bloqueo de puertos TCP/UDP. Esto impide el acceso a ciertas aplicaciones dentro de una red, manteniendo públicos sólo los servicios que deben serlo. Para esto CIISTEC abre o cierra los puertos que sean necesarios de acuerdo a las políticas de seguridad definidas previamente por el Suscriptor.

La creación de una red interna, que sólo permitirá la conexión de los usuarios de acuerdo con las políticas que el Suscriptor determine en conjunto con CIISTEC.

Opcionalmente a solicitud expresa del Suscriptor, la instalación de un antivirus en el firewall para prevenir posibles contaminaciones por virus electrónicos procedentes de Internet. Como el antivirus se instala en el equipo firewall, el equipo no tiene posibilidad de detectar y filtrar infecciones de virus que sean introducidos por algún medio diferente a la red (floppy disk, CD, USB Memories, etc), por lo que dicha contaminación queda excluida de los alcances del servicio iSourcing Seguridad.

El Suscriptor podrá solicitar la configuración de VPN’s punto a punto en el firewall administrado por CIISTEC para hacer túneles a través de Internet, permitiendo la conexión con otros firewall’s, siempre y cuando el equipo sea compatible con el proporcionado por CIISTEC.

CIISTEC instalará el firewall en las oficinas de Suscriptor previo estudio de las políticas de seguridad actuales del Suscriptor para recomendar mejoras a las mismas de acuerdo a las mejores prácticas de seguridad informática. Una vez definidas las políticas de seguridad por el Suscriptor (en base al número de puerto TCP/UDP utilizado por el servicio), CIISTEC será responsable de aplicarlas en el firewall.

Una vez generada la política y aplicada en el firewall, la renta mensual cubre la realización de cambios en las políticas hasta un número máximo de 5 eventos, después de los cuales se tendrá un costo adicional por

El servicio de HiperBlindaje creará una red interna y el equipo funcionará como un punto de control para el acceso hacia y desde Internet, estableciendo Políticas de Conexión de la red Interna a Internet y viceversa.

Para determinar conjuntamente las políticas de seguridad a establecer en el firewall, personal de CIISTEC programará hasta dos sesiones de trabajo con el Suscriptor de un máximo de 4 horas en día y horas hábiles, de manera que el Suscriptor podrá definir los servicios que desea que entren/salgan de su red.

Una vez implementadas las políticas que sean definidas, el servicio será administrado y monitoreado por CIISTEC de manera centralizada y remota, generalmente CIISTEC no tendrá que desplazar a su personal a las oficinas del Suscriptor.

Limitaciones

Este servicio esta destinado para Suscriptores que se encuentran dentro de la red de datos de CIISTEC, cuyo servicio sea entregado en RJ-45 y/o que sean alcanzables a través de protocolo IP.

El establecimiento de las políticas en el firewall se debe de realizar en conjunto con el Suscriptor y éste debe de conocer los servicios que se manejan en su red. Si lo anterior no sucede se tendrán políticas estándares aunque éstas serán limitadas.

CIISTEC no será responsable de proteger los ataques relacionados con la falta de instalación de algún parche en el (los) servidor(es) del Suscriptor. En ningún caso CIISTEC será responsable de pérdidas de información, accesos no autorizados o de virus propagados dentro de la red del Suscriptor, dada la cantidad de formas conocidas y por conocerse para atacar una red desde Internet, así como la aparición continua de virus nuevos.

CIISTEC no será responsable de ningún tipo de daños y perjuicios que pudiese sufrir el Suscriptor, pérdidas totales o parciales, corrupción de archivos o cualquier otro tipo de afectación a la información y/o programas de cómputo y/o aplicaciones que el Suscriptor tenga en sus servidores, computadoras o cualquier otro dispositivo. Será responsabilidad del Suscriptor el realizar los respaldos que sean necesarios para resguardar la información.

Asimismo, queda expresamente entendido que CIISTEC no será responsable en ningún caso del pago de los

daños y perjuicios que se pudieren ocasionar al Suscriptor con motivo de cualquier tipo de interrupción o falla de los servicios, quedando limitada su responsabilidad al acreditamiento o descuento en el pago de la renta de la parte proporcional por el tiempo en que el Suscriptor no haya tenido a su disposición el Servicio por causas imputables a CIISTEC,

Los servicios de seguridad comprendidos en este anexo excluyen la seguridad de cualquier aplicación y equipos para servicios de telefonía y cualquier otra aplicación bajo el control del Suscriptor, por lo que el Suscriptor asume cualquier responsabilidad por el uso de su aplicación y equipos de telefonía.

En caso de que alguna de las fallas en el servicio se produjera por mal manejo del equipo por parte del Suscriptor, CIISTEC quedará liberada de toda responsabilidad.

En ningún caso CIISTEC será responsable del análisis ni almacenamiento de Logs (registros) que genere el firewall. SEXTA.-

Reparación o reemplazo de equipo:

El equipo que CIISTEC instala para proveer el servicio de seguridad contará con una póliza de servicio de mantenimiento remoto y reemplazo avanzado que es proporcionado por el fabricante a través de CIISTEC, la cual tendrá la vigencia del contrato de iSourcing Seguridad.

El tiempo de reemplazo del equipo en sitio dentro de la Ciudad de México, Guadalajara y Monterrey es de 12 horas hábiles a partir de que CIISTEC determine que el equipo es inoperante para brindar el servicio. En localidades foráneas el equipo se enviará por el medio elegido por CIISTEC y el tiempo de reemplazo será de 12 horas, más el tiempo que el medio elegido tarde en llegar al lugar.