**POLÍTICAS DEL SERVICIO DE CERTIFICADOS DE SEGURIDAD SSL.**

Políticas en vigor a partir del 07 de Noviembre de 2020.

## 1. DEFINICIONES.

Los términos definidos en esta sección podrán ser utilizados en las presentes políticas tanto en singular como en plural.

Los términos referidos en mayúsculas y sin definición en las presentes políticas, tendrán la definición y sentido que les haya sido otorgado en las Políticas de Nombres de Dominio Akky, a no ser que en las presentes se definan de otra manera o se limite dicha definición o sentido.

Todos los encabezados utilizados en las presentes políticas se utilizan exclusivamente para facilitar su lectura, pero no se tomarán en cuenta al realizar la interpretación de las mismas.

1.1. ***Algoritmo de Firma***
Es un método para cifrar información mediante funciones matemáticas, los algoritmos 'hash' transforman un conjunto de datos en un único valor de longitud fija que al ser calculado es utilizado para verificar la integridad de la información almacenada.

1.2. ***Autoridad Certificadora***.
Empresa encargada de la validación y emisión de los Certificados SSL. La Autoridad Certificadora varía dependiendo de la marca del certificado adquirido, en el caso de los certificados de tipo Validación de Dominio y Validación Extendida es Sectigo® (antes Comodo®) quien realiza la verificación correspondiente mediante los documentos que determina como válidos. El caso de los certificados de tipo Validación de la Organización, Digicert® es quien efectúa la verificación a través de los documentos que determina como válidos para este fin.

1.3. ***Certificado SSL (Secure Sockets Layer)***.
Es un título digital que autentifica la identidad de un sitio web y cifra la información que se envía al servidor.

1.4. ***Contacto Administrativo***.
Este contacto principal será el solicitante oficial del certificado y debe ser un empleado que esté disponible para responder cualquier pregunta relacionada con el proceso de validación.

1.5. ***Contacto Técnico***.
Este contacto recibirá el certificado y es generalmente quien instalará el certificado en el servidor web.

1.6. ***CSR (Certificate Signing Request)***.
Es un archivo con texto cifrado que contiene la información de la petición del certificado SSL entre la que se encuentra el nombre del dominio, nombre de la organización, etc.

1.7. ***Indicador de Confianza para Sitio Web***
Es un elemento que se utiliza en los Certificados SSL para acompañar al Sitio Web y la forma en que es presentado puede variar dependiendo del navegador utilizado. Ejemplos: https, el icono del candado en la barra del navegador, un sello del sitio de una autoridad certificadora, una barra verde que envuelve la URL en certificados de Validación Extendida.

1.8. ***IP Dedicada o Estática.***
Dirección asignada por un proveedor de servicios de Internet de forma permanente a un dispositivo.

1.9. ***Mecanismos de Verificación***
Son utilizados por la Autoridad Certificadora para probar que el usuario es el propietario del dominio o que tiene derechos sobre el mismo. Por ejemplo: Correo electrónico, Archivo HTTP, Archivo HTTPS, Registro Cname.

1.10. ***Modalidad de Certificados SSL.***
Los Certificados SSL, pueden ser emitidos para un Nombre Común, para los diferentes subdominios derivados del Nombre Común o para múltiples Nombres de Dominio independientes entre sí.

1.11. ***Nombre Común.***
Es la industria de los Certificados SSL, se le denomina así al Nombre de Dominio incluido en CSR.

1.12. ***SANS (Secure Alternate Name).***
Nombres de dominios y subdominios adicionales que pueden agregarse a un certificado multidominio.

1.13. ***Servicio.***
Se refiere al Certificados de Seguridad SSL.

1.14. ***Solicitante.***
El Usuario que haya realizado la contratación del Servicio a través del Sistema.

1.15. ***Tipos de Certificados SSL***
Existen 3 tipos de Certificados SSL, que se pueden emitir:

a. Validación de Dominio. La Autoridad Certificadora, valida la propiedad del Nombre de Dominio relacionado.
b. Validación de la Organización. La Autoridad Certificadora, valida la propiedad del Nombre de Dominio relacionado, y verifica el nombre de la organización y teléfono.
c. Validación Extendida. La Autoridad Certificadora, valida la propiedad del Nombre de Dominio relacionado, y verifica el nombre de la organización, teléfono, dirección física y en buenos términos legales.

## 2. DISPOSICIONES GENERALES.

El Registrante y los Usuarios de un Nombre de Dominio en Akky manifiestan que conocen y aceptan las presentes políticas, con relación a este Servicio, al Servicio de Nombres de Dominio y los términos y condiciones establecidos por la Autoridad Certificadora (Sectigo® y Digicert®) para la emisión, revocación y administración de un Certificado SSL; así como la facultad de Akky para eliminarlas y/o modificarlas en cualquier momento.

Cualquier modificación o actualización a las Políticas publicadas en el Sitio Web de Akky se dará a conocer mediante un aviso de al menos cinco (05) Días inmediatos anteriores a la fecha de su entrada en vigor, en el Sitio Web de Akky, con objeto de que el Registrante y los Usuarios manifiesten lo que a sus intereses convenga. Una vez transcurrido el plazo anterior el Registrante y los Usuarios del Nombre de Dominio quedarán obligados bajo estas nuevas Políticas, sin que sea necesario que Akky realice ningún otro tipo de publicación o aviso.

Akky podrá ceder, transferir, comprometer, traspasar o enajenar, total o parcialmente, los derechos y obligaciones derivados de la prestación del Servicio contenido en los términos y condiciones de las presentes Políticas, sin previa autorización. En caso de llevarse a cabo alguno de los anteriores supuestos, Akky comunicará el nuevo responsable de la ejecución adecuada y oportuna de las actividades relativas a la prestación del presenta Servicio, por lo que el Solicitante, los Usuarios y/o en su caso el Registrante, quedarán sujetos a los términos y condiciones establecidos en las Políticas del nuevo responsable.

Akky simplemente administra el espacio de Nombres de Dominio, y por tanto, cualquier consecuencia derivada del registro y/o uso del Servicio y/o de los Nombres de Dominio que constituya o pudiera constituir violaciones a la legislación aplicable, es responsabilidad exclusiva del Registrante, aún y cuando el Nombre de Dominio con el que se configura este Servicio sea administrado con otro Registrar.

Akky se reserva el derecho de revisar, remover, editar o bloquear cualquier material o información que los Usuarios hayan publicado, recibido o enviado en contravención a alguna ley, por solicitud expresa de una Autoridad o en caso de abuso del Servicio. Akky, en cualquier momento, podrá suspender, temporal o permanentemente, y/o cancelar el acceso y/o el uso del Servicio.

## 3. DEL SERVICIO.

3.1. ***Generalidades***.

3.1.1. ***Contratación***.

El Servicio puede ser contratado por los Usuarios a través del Sistema al realizar la selección de un Tipo de Certificado SSL y agregarlo al carrito de compra, el Solicitante es responsable de obtener la autorización del Registrante para relacionar este Servicio con un Nombre de Dominio, el cual puede ser administrado incluso con otro Registrar.

3.1.2. ***Vigencia***.

El Solicitante escogerá el periodo de cobertura del Servicio de acuerdo con las opciones que determine el Sistema. La vigencia del Servicio iniciará en la fecha en que el Certificado SSL haya sido emitido por la Autoridad Certificadora. Es necesario que se realice la configuración y validación para que la Autoridad Certificadora emita el certificado, en caso contrario, éste expirará sin haber sido emitido al cumplir el plazo seleccionado.

3.1.3. ***Renovación***.

Para la renovación de un Certificado SSL, Akky podrá notificar al Solicitante 30 días antes de la fecha de vencimiento del certificado. El envío de esta notificación se realiza como apoyo al Solicitante para la reemisión del certificado, por lo cual es responsabilidad de éste conocer la fecha de vencimiento y efectuar la reemisión en tiempo y forma. Una vez recibido el aviso de próximo vencimiento y antes de que concluya el periodo de vigencia seleccionado por el Solicitante en la contratación del Servicio éste deberá renovarlo por los periodos determinados por el Sistema, de su elección. Es responsabilidad del usuario realizar la renovación del Certificado SSL antes de su vencimiento, ya que una vez que ha concluido el periodo de vigencia, el Servicio es considerado como expirado, por lo que es necesario que la Autoridad Certificadora valide y emita el Certificado SSL nuevamente como en la contratación.

3.1.3.1. En la industria de los Certificados SSL, es necesario que se realice la reemisión de un Certificado SSL para aquellos casos en que la cobertura contratada sea mayor a un (1) año, considerando lo siguiente:

3.1.3.1.1. La reemisión debe realizarse por el usuario a partir de 30 días previos a la fecha de expiración del certificado.

3.1.3.1.2. Al reemitirse un certificado, la Autoridad Certificadora se reserva el derecho de efectuar nuevamente la verificación de la documentación, en los casos donde existiera la actualización de parte la información contenida en el CSR.

3.1.3.1.3. Al realizar la reemisión debe conservarse el Nombre Común, contenido en el CSR.

3.1.3.1.4. El aviso correspondiente será enviado 30 días antes de concluir el período de vigencia.

3.1.4. ***Asignación***.

El Servicio será emitido para el o los Nombre(s) de Dominio o subdominios señalado(s) por el Usuario, al realizar su configuración a través del Sistema, por lo que, para poder efectuar la asignación de este servicio y su correcto funcionamiento, el Solicitante asume las siguientes responsabilidades:

3.1.4.1. La elección del tipo de certificado y mecanismo de verificación seleccionado y su configuración.

3.1.4.2. Asegurar que cuenta con la documentación y requisitos establecidos para que la Autoridad Certificadora, valide y emita el Certificado SSL seleccionado. Para los tipos de certificado de Validación de Organización y Validación Extendida el Solicitante deberá asegurar que el Contacto Administrativo, provea los documentos requeridos y realice el registro en los Directorios de Información que la Autoridad Certificadora especifique. Por lo que exime de cualquier tipo de responsabilidad a Akky en caso de que esta autoridad determine la imposibilidad de emitir el Certificado SSL por incumplimiento de los mismos.

3.1.4.3. Debe asegurar que el Nombre de Dominio relacionado con este Servicio exista y cuente con cobertura pagada con el Registrar que corresponda.

3.1.4.4. Realizar la configuración solicitada por la Autoridad Certificadora dependiendo del mecanismo de verificación seleccionado.

Notificar a los contactos indicados en los datos del certificado como Contacto Administrativo y/o Contacto Técnico.

3.1.4.5. Asegurar que el Contacto Administrativo del Certificado realice la validación de la propiedad del Nombre de Dominio para todos los tipos de Certificados SSL.

3.1.4.6. Akky se reserva el derecho de modificar o eliminar la asignación del Servicio a solicitud del Registrante de un Nombre de Dominio posterior a realizar la validación de la Titularidad y de la autenticación del Registrante, mediante la presentación de la documentación requerida o suficiente para este fin.

3.1.5. ***Cancelación***.

3.1.5.1. El Solicitante puede llevar a cabo la cancelación del Servicio una vez que haya sido emitido, la cual se podrá realizar en cualquier momento por medio del Sistema.

3.1.5.2. Akky se reserva el derecho de eliminación del Servicio de conformidad con el punto 3.1.4.6. de las presentes políticas.

3.1.5.3. La Autoridad Certificadora, podría notificar al usuario, algún detalle de seguridad encontrado en el Sitio Web relacionado con un Certificado SSL, el cual es necesario que sea resuelto para continuar con la validez del certificado. En caso de no ser atendida esta comunicación, la Autoridad Certificadora podría revocar el Certificado SSL. Es responsabilidad del Solicitante y los Usuarios, atender la comunicación de la Autoridad Certificadora, a fin de conservar su Certificado SSL vigente por lo que exime a Akky de subsanar su revocación.

3.1.5.4. En el caso de cancelación del Servicio, el pago del mismo no será reembolsable ni transferible.

3.1.6. ***Eliminación***.

3.1.6.1. El Servicio será eliminado al no ser recibido el pago dentro de los períodos establecidos por Akky, al momento de la contratación del Servicio o en la fecha de su renovación.

3.1.7. ***Acceso***.

Para tener acceso y configurar el Servicio, el Solicitante deberá utilizar su Cuenta de Usuario en el sistema de Akky.

3.1.8. ***Tarifas, Plazos y Formas de Pago***.

3.1.8.1. Las tarifas y las formas de pago por la prestación del Servicio serán mostradas al usuario antes de concluir el pago de su compra o renovación, en el resumen del carrito.

3.1.8.2. El Solicitante y los Usuarios deberán cubrir la tarifa que corresponde al Servicio indicado conforme al periodo de cobertura.

3.1.8.3. El Solicitante y los Usuarios reconocen y aceptan que los pagos realizados no son reembolsables ni transferibles a otro Servicio. Adicionalmente, si se solicita la cancelación del Servicio o la Autoridad Certificadora determina la imposibilidad de emitir el certificado SSL de conformidad con el punto 3.1.4.2., el costo del mismo tampoco será reembolsable ni transferible.

3.1.8.4. Akky podrá enviar diversos avisos relativos al cobro del Servicio antes de su fecha de vencimiento, vía correo electrónico al Solicitante. El envío de estos mensajes se realiza como apoyo a los Usuarios para el pago del servicio por lo cual es responsabilidad de los mismos conocer la fecha de renovación del Servicio y efectuar el pago en tiempo y forma.

3.1.8.5. A partir de la fecha de contratación del Servicio el Usuario cuenta con el período de vigencia indicado en la Orden de Servicios para realizar el pago del mismo.

3.1.8.6. Al generar la Orden de Servicios mediante tarjeta de crédito o tarjeta de débito, Akky habilitará, la renovación automática para los servicios incluidos en esa Orden de Servicios. Si el usuario conserva la renovación automática se generará un cargo transitorio para confirmar que la tarjeta es válida, mismo que será devuelto una vez que se concluye esa validación. Es responsabilidad del Usuario Principal y/o Usuarios con permisos de Pago según corresponda, colocar información correcta y asegurar que mediante este método el pago que la renovación de esos servicios pueda concretarse. En caso de ser necesario Akky notificará a los usuarios, que no fue posible procesar la renovación automática a fin de que se verifiquen la información colocada. Si no se realiza dicha modificación los servicios serán colocados en el estatus correspondiente por no haber sido posible procesar su renovación.

3.1.8.7. La renovación automática, podrá ser inhabilitada al momento de la generación de la Orden de Servicios o mediante el Panel de Control, por el Usuario Principal y/o los Usuarios de Pago, sin embargo, será necesario, generar la Orden de Servicios correspondiente para su renovación. En caso de modificar la tarjeta de crédito o débito se generará un cargo transitorio para confirmar que la tarjeta es válida, mismo que será devuelto una vez que se concluye esa validación.

3.1.8.8. Para efectuar el procesamiento de la renovación automática Akky utilizará los servicios de Openpay® como operador de estos pagos de tarjetas de crédito y tarjetas de débito.

3.1.8.9. Existe un plazo de hasta 30 (treinta) días naturales posteriores a la fecha de Renovación del Servicio para realizar el pago correspondiente.

3.1.8.10. La contraprestación del Servicio será proporcional al tiempo de vigencia contratado.

3.2. ***Especificaciones***.

3.2.1. El Servicio consiste en establecer una conexión segura a través de la transferencia de datos cifrados entre un navegador y un servidor web. Existen diferentes Tipos y Modalidades de Certificados SSL cada uno con características específicas, mismos que son publicados mediante el Sitio Web de Akky.

3.2.2. La validación de la información necesaria para la emisión del Certificado SSL dependiendo de su Tipo, es efectuada mediante una Autoridad Certificadora determinada por la marca que emite el certificado, la cual establecerá comunicación con el Contacto Administrativo vía correo electrónico y/o telefónica. La Autoridad Certificadora se reserva el derecho de utilizar el idioma de origen con el cual establecerá su comunicación. Akky podría apoyar al Contacto Administrativo, en el entendimiento de la validación por la Autoridad Certificadora, en caso de que esta utilice un idioma diferente al de español.

3.2.3. Akky se reserva el derecho de brindar el Servicio con recursos propios o bien con el apoyo de proveedores.

3.2.4. Los Usuarios aceptan que son mayores de edad y están en pleno uso y goce de su capacidad de ejercicio, en caso contrario debe abstenerse de utilizar y/o solicitar el Servicio.

3.2.5. El Servicio se asocia a uno o más Nombres de Dominio o subdominios dependiendo de la Modalidad del Certificado y dicho Servicio no será transferible a ningún otro Nombre de Dominio.

3.2.6. La configuración del Servicio se realiza de la siguiente forma:

3.2.6.1. Ingreso y verificación del CSR. Es necesario que después de haber ingresado en el Panel de Control, el usuario coloque el CSR correspondiente en la sección de Generar certificado. Una vez que ha validado el CRS, es necesario que la información contenida en él sea verificada.

3.2.6.2. Configuración. En el caso de que el Certificado SSL sea multidominio, es necesario que se enlisten los Nombres de Dominio o subdominios que serán amparados por este certificado. Es responsabilidad de quien realiza esta configuración colocar en este paso los Nombres de Dominio, ya que, en caso de no hacerlo, se deshabilitará la compatibilidad con SAN y no sería factible utilizar esta modalidad.

3.2.6.3. Selección del tipo de servidor. Es necesario seleccionar el tipo de plataforma de servidor configurado para el Certificado SSL, en caso de quien realice la configuración desconozca esta información y continúe con la configuración por defecto en el proceso de configuración, el Certificado será emitido considerando el formato estándar X 509 (PEM por sus siglas en inglés Privacy Enhanced Mail), el cual es un estándar UIT-T (Por sus siglas Unión Internacional de Telecomunicaciones) para infraestructuras de claves públicas.

3.2.6.4. Elección del Mecanismo de Verificación. Dependiendo del Tipo y marca del Certificado el Mecanismo de Verificación podría variar, los tipos de Mecanismos de Verificación son: Correo electrónico, Archivo HTTP, Archivo HTTPS, Registro Cname.

3.2.6.5. Selección del Algoritmo de Firma. Dependiendo del Tipo y marca del Certificado el Algoritmo de Firma podría variar, las opciones son: SHA-256, SHA-384, SHA-512.

3.2.6.6. Información de los Contactos Administrativo, Técnico. Es necesario que se indique datos de contacto para que la Autoridad Certificadora, se comunique con el Contacto Administrativo, en caso de ser necesario para llevar a cabo la validación de la

información, y en el caso del Contacto Técnico para el envío del archivo que contiene el Certificado emitido vía correo electrónico.

3.2.6.7. Datos de la Organización. Dependiendo del Tipo de Certificado podría ser necesario ingresar la información solicitada de la Organización relacionada con el Certificado SSL, el Solicitante es responsable de que la información proporcionada, coincida con los detalles legales registrados de la empresa a la documentación. En caso de ser incorrecta, podría ocurrir la demora o la imposibilidad de emitir el Certificado SSL.

3.2.7. Al concluir la configuración para emitir el certificado, será necesario realizar las instrucciones enviadas por correo electrónico de parte de la Autoridad Certificadora dependiendo del Tipo Mecanismo de Verificación seleccionado.

3.2.8. Es necesario que el Solicitante considere para la instalación de un Certificado SSL el utilizar una IP estática.

3.2.9. En caso de requerir hacer efectiva la garantía relacionada con Certificado SSL, es necesario que el Solicitante se remita al proceso establecido por la Autoridad Certificadora (Sectigo® y Digicert®).

3.3. ***Propiedad Intelectual.***

El Registrante y los Usuarios deben asegurarse que no están violando algún derecho de propiedad intelectual o industrial al hacer uso del Servicio (tales como: marca registrada, avisos comerciales, reservas de derechos), y/o cualquier otro derecho de tercero, en relación con el ordenamiento jurídico nacional e internacional aplicable en la materia.

3.4. ***Datos personales.***

El Registrante y los Usuarios son los únicos responsables por el tratamiento que realicen de los datos personales a los que tengan acceso en virtud del uso del Servicio, así como de su protección y que su tratamiento se realice con el sigilo y seguridad que ameriten, de conformidad con lo estipulado en la Ley Federal de Protección de Datos en Posesión de Particulares, así como la legislación vigente que resulte aplicable en la materia.



Eugenio Garza Sada 427 L- 4, 5 y 6, Col. Altavista, Monterrey, Nuevo León, CP 64840
**Monterrey, México:** 8864-2626 **Interior de la República: (**81) 8864-2626 **Extranjero:** +52(81) 8864-2626
www.akky.mx