FIRMA DIGITAL Y CIPE

FIRMA DIGITAL
Y CIPE

Universidad de LA PUNTA

GOBIERNO DE SAN LUIS | SAN LUIS NOS UNE

FIRMA DIGITAL Y CIPE

Universidad de LA PUNTA

GOBIERNO DE SAN LUIS

SAN LUIS NOS UNE

Gobernador
Alberto José Rodríguez Saá

Ministra de Ciencia y Tecnología
y rectora de la Universidad de La Punta
Alicia Bañuelos

Jefe de Programa CIPE
Nicolás Rodríguez Iannello

Directora de Instituto Firma Digital San Luis
Luciana Rosario Vera

ÍNDICE

7 **PRÓLOGO** por Alberto Rodríguez Saá

9 **PRÓLOGO** por Alicia Bañuelos

1 **INTRODUCCIÓN** 13

2 **CONCEPTOS BÁSICOS DE FIRMA DIGITAL** 19

3 **IMPLEMENTACIÓN DE LA FIRMA DIGITAL EN SAN LUIS** 39

4 **POLÍTICAS DE CERTIFICACIÓN** 45

5 **RÉGIMENES DE AUDITORÍAS** 55

6 **INFRAESTRUCTURA TECNOLÓGICA DE LA FIRMA DIGITAL EN SAN LUIS** 69

7 **SEGURIDAD Y REDUNDANCIA DE LA FIRMA DIGITAL EN SAN LUIS** 75

8 **CÉDULA DE IDENTIDAD PROVINCIAL ELECTRÓNICA** 79

9 **INFRAESTRUCTURA Y CENTROS DE EMISIÓN. CANTIDAD Y DISTRIBUCIÓN** 75

10 **DE CIPE 2.0 A CIPE 4.0** 75

11 **FUNCIONALIDADES DE CIPE** 75

12 **CERTIFICACIONES INTERNACIONALES** 75

13 **CRÉDITOS** 75

Alberto Rodríguez Saá

Gobernador
de la Provincia de San Luis

PRÓLOGO

Gobernador
de la Provincia
de San Luis

A todos los puntanos, hoy nos produce un enorme orgullo que San Luis sea el Estado más digital del mundo, en un escenario global atravesado por la Cuarta Revolución Industrial.

Esta Cuarta Revolución Industrial está definida por tecnologías de vanguardia destinadas al desarrollo de sociedades cuyas demandas son cada vez más complejas. Incluye la robótica, la inteligencia artificial, las cadenas de bloques, la biotecnología y la internet de las cosas, entre muchas otras.

Cuando diseñamos nuestra Agenda Digital, hace más de dos décadas, estábamos tomando un atajo al futuro, a este presente y a este escenario. Pero alcanzarlo era un desafío enorme.

Partimos desde la Inclusión Digital, de la periferia al centro. Internet gratis, entrega de dispositivos, formación de excelencia, creación del Derecho Humano de Cuarta Generación de acceso libre y gratuito a Internet, incluido en la Constitución Provincial.
Enormes hitos.

La ***Firma Digital y la CIPE***, son iniciativas que forman parte de la Agenda Digital. Presentes cada día no solo para lograr un Gobierno más eficiente, más saludable con el medio ambiente por el ahorro de papel, sino para cada habitante de San Luis que necesite demostrar su identidad digital.
Herramientas que nos permitieron alcanzar y superar los objetivos.

Por lo tanto, la celebración es no sólo por este estatus de privilegio a nivel global, también lo es por el camino recorrido.

Alicia Bañuelos

Rectora de la Universidad de La Punta y Ministra de Ciencia y Tecnología de San Luis

PRÓLOGO

Rectora de la Universidad de La Punta y Ministra de Ciencia y Tecnología de San Luis

San Luis abordó la inclusión digital a partir de tres pilares: dispositivos, conectividad y formación. El desafío era lograr que cada habitante de la Provincia accediera a estos tres ejes, para ser auténticamente democráticos e inclusivos.

La decisión de crear nuestra propia infraestructura de clave pública, fue impulsada por un escenario provincial propicio para poner en funcionamiento en poco tiempo una Administración Digital.

Todas las dependencias del estado estaban conectadas a internet, entregábamos dispositivos a la sociedad y existían proyectos de capacitación en el uso de herramientas digitales que estaban en total ejecución y con los años se irían incrementando.

En términos prácticos, la iniciativa de Firma Digital permitió un ahorro de más del 85% en papel, para la administración pública.

Y la CIPE es una herramienta cotidiana en la vida de miles de puntanos, permitiéndoles acreditar su identidad en forma digital.

Iniciativas exitosas de la Agenda Digital, que llevamos adelante desde hace más de dos décadas.
Ésta es la historia de la CIPE y la Firma Digital.

CIPE 3.0
FRANCO
11 FEB 19
11 FEB 29
FIRMA TITULAR

1 INTRODUCCIÓN

INTRODUCCIÓN

Contar con una infraestructura de firma digital sólida que pudiera responder a cada una de las necesidades y proyectos del gobierno provincial fue uno de los objetivos planteados por San Luis en el año 2006. A partir de ese entonces se trazó un plan para, como primera medida, dictar la normativa jurídica que le diera validez, construir la sala cofre que alojaría la infraestructura, adquirir el equipamiento informático y planificar la estrategia de su funcionamiento. Construimos la infraestructura de firma digital de San Luis pensando en su utilidad, las facilidades que ofrecería a los distintos sectores de la sociedad y así se fueron delineando los distintos planes. Entre ellos, CIPE (Cédula de Identidad Provincial Electrónica), una herramienta esencial en el vínculo con cada ciudadano.

Como toda innovación tecnológica debió superar la resistencia de muchos sectores de la población. Con el esfuerzo dedicado a su implementación, el impulso en su promoción y la confianza de quienes comenzaron a usarla; hoy la CIPE forma parte de la vida cotidiana de San Luis, ofreciendo soluciones en el día a día de los ciudadanos.

Todo ello se pudo realizar gracias a la visión estratégica de Alicia Bañuelos, quien era la Rectora de la Universidad de La Punta, institución encargada de la estrategia digital provincial, y la visión y el respaldo del entonces Gobernador de la provincia, Alberto Rodríguez Saá.

AGENDA DIGITAL DE SAN LUIS

San Luis cuenta con una agenda digital en ejecución desde hace más de veinte años.

En 1998, cuando poco más del 3 por ciento de la población mundial tenía acceso a Internet, el gobierno de San Luis comenzó su proceso pionero de digitalización. La gobernación puntana desplegó la infraestructura física y legal de la Autopista de la Información. La AUI es una red de banda ancha que conecta a todas las localidades de más de veinte habitantes y un Data Center de clase mundial. En la actualidad esta red cuenta con 7000 KM de fibra óptica, provee internet gratuita a toda la población. La misma fue construída acercando cada localidad provincial de la periferia al centro (años 1998 – 2005).

En una segunda etapa San Luis consagró la inclusión digital como un derecho humano de cuarta generación en la Constitución provincial, y se sentaron las bases de la comunidad digital puntana mediante la convergencia entre gobierno, comunidad científica y tecnológica, industria, y sociedad.

En una tercera etapa, iniciada en 2015, ha puesto la tecnología al servicio de la vida, democratizando el acceso a los dispositivos, la conectividad y la formación del futuro, con el afán de posicionar a San Luis entre los pueblos pioneros que producen tecnología, y no sólo la consumen.

San Luis buscó superar la agenda digital de mínima a la que se limitaba la inmensa mayoría de los gobiernos: la reducción de la denominada "brecha digital" (el porcentaje de ciudadanos sin acceso a Internet).

Hablar de "inclusión digital", en cambio, suponía motorizar

una agenda superadora, en evolución permanente, para construir el estado de bienestar del siglo XXI. La noción básica de la inclusión digital, repetida por muchos gobiernos como una consigna vacía, era que los pueblos sin conectividad padecerían una desventaja central en el acceso al conocimiento y su producción. Pero sin dispositivos mediante los cuales acceder a los contenidos que ofrecía la red, y sin el conocimiento acerca de cómo utilizar los dispositivos y la propia conectividad, la digitalización nunca sería una tecnología disruptiva o democrática. Porque nadie la adoptaría, y porque reproduciría la inequidad en lugar de reducirla.

Desde entonces, San Luis entiende la "inclusión digital" como una política con tres pilares: dispositivos, conectividad y formación. Sólo el acceso a los tres es auténticamente disruptivo y democrático. En cada uno de los tres pilares los puntanos íbamos a hacer la diferencia. En cuanto al servicio de conectividad, el primer paso fue la realización de estudios para llevar conectividad gratuita a todo el territorio. Luego se instalaron antenas en veinticuatro localidades y se brindó conectividad gratuita a las ciudades más pobladas de la provincia: San Luis y Villa Mercedes. El objetivo desde entonces sería llegar a todos los pueblos con al menos veinte habitantes, una meta inimaginable desde la lógica del mercado.

De hecho, en la Argentina las empresas prestadoras de Internet tienen obligación contractual de dar servicio a ciudades de por lo menos 50.000 habitantes. En cuanto a la política de acceso gratuito a los dispositivos digitales, esta evolucionó con el tiempo.

Sobre la base de dichos pilares, San Luis decidió construir su propia infraestructura de firma digital para, en una primera etapa, acercar la administración pública a sus ciudadanos, otorgándoles además un dispositivo criptográfico que pudieran obtener de manera gratuita, la Cédula de Identidad Provincial Electrónica (CIPE).

02
CIPE 4.0
CÉDULA DE IDENTIDAD
PROVINCIAL ELECTRÓNICA

2

CONCEPTOS BÁSICOS DE FIRMA DIGITAL

MINISTERIO
DE CIENCIA
Y TECNOLOGÍA

AGENDA DIGITAL DE SAN LUIS

A continuación se expresan conceptos básicos acerca de firma digital y firma electrónica para facilitar la comprensión de la herramienta adoptada en la provincia.

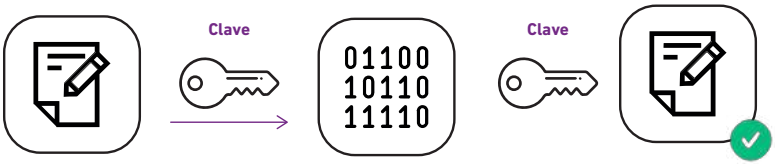
Hasta no hace mucho tiempo cuando hablábamos de documentos pensábamos inmediatamente en “papeles” y concebíamos como única forma de asumir un compromiso aquello que volcábamos en soporte papel. Sin embargo los avances tecnológicos y el aumento de los negocios celebrados entre personas que se encuentran en distintas ciudades, o inclusive en diferentes países, nos llevaron a incluir en la noción de documentos también a aquellos que pueden estar en otros soportes. Pero por si solo otorgarle valor jurídico a los documentos digitales no resuelve todas las cuestiones o dudas que podrían derivar de lo acordado por este medio, ya que es necesario saber quién es el autor de ese documentos, o mejor dicho, quien se compromete a lo expresado en el texto de ese documento digital y además tener la certeza que desde que el emisor expresó esa voluntad hasta que el receptor efectivamente recibió el documento digital, esa expresión de voluntad no ha sido modificada o adulterada.

Justamente, la Firma Digital es una herramienta tecnológica que utilizando criptografía de clave pública permite verificar la identidad del autor de un documento y garantizar la integridad de su contenido.

CRIPTOGRAFÍA DE CLAVE PÚBLICA

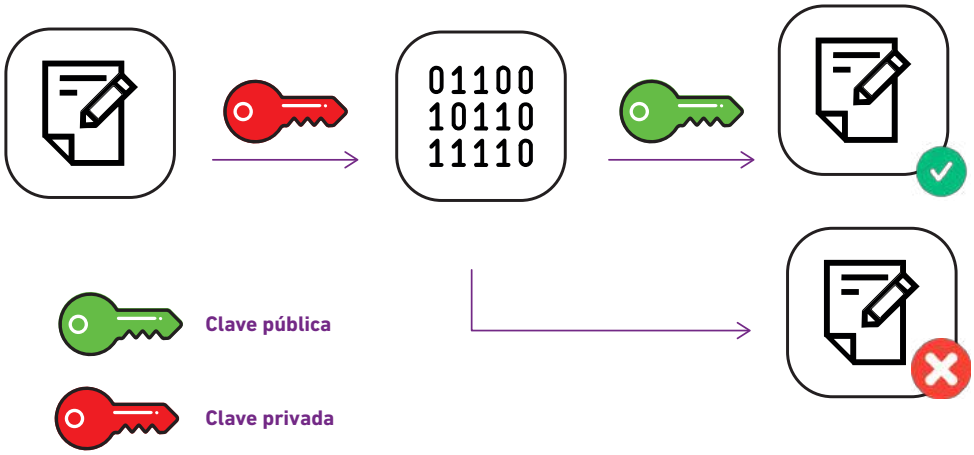
Existen muchos tipos de criptografía, pero para comprender el tema en cuestión sólo dos tipos son relevantes: Criptografía de clave simétrica y Criptografía de clave asimétrica.

La criptografía de clave simétrica se basa en el uso de una misma clave para cifrar y descifrar los datos de un mensaje o documento. Esta clave debe ser conocida por todos los participantes de la comunicación: emisor y receptor, y debe mantenerse en secreto para que sólo los participantes puedan acceder el contenido del mensaje. La ventaja de este método es que es muy rápido y eficiente ya que ambas partes sólo necesitan conocer esa única clave para leer el contenido del mensaje, pero su gran desventaja reside en la distribución y el almacenamiento de la clave, ya que puede ser vulnerables a ataques.



La criptografía de clave asimétrica, también llamada de clave pública, se basa en el uso de un par de claves que son diferentes entre sí pero se encuentran relacionadas matemáticamente: una clave pública y una clave privada que se corresponden. La clave pública se puede compartir con cualquier persona, mientras que la clave privada se debe guardar en un lugar seguro, debe ser de exclusivo conocimiento de su titular. La información que es cifrada con la clave pública sólo puede ser descifrada con la clave privada, y correlativamente, la información que es

cifrada con la clave privada sólo acepta el procedimiento inverso con la correspondiente clave pública. La ventaja de este método es que no requiere un canal seguro para intercambiar las claves ya que sólo será necesario hacer pública la clave pública, mientras que la privada debe ser conservada por su titular. La desventaja, si hubiera que señalar alguna, es que se trata de un procedimiento más lento y complejo que el simétrico.



FUNCIONES HASH

Una función criptográfica hash es un algoritmo matemático que transforma un mensaje de datos en un número hexadecimal de longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida siempre tendrá la misma longitud.

Entonces en criptografía, el hash es una forma de resumir un mensaje o un archivo en un valor único y fijo, llamado hash o digesto. El hash se calcula aplicando una función matemática sobre el mensaje o el archivo, de forma que cualquier cambio en el contenido producirá un cambio en el hash.

FIRMA DIGITAL EN LA LEY ARGENTINA

En concordancia con lo detallado ut supra la Ley Nacional de Firma Digital, N° 25.506, establece que

"Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma".

Cuando una persona quiere firmar digitalmente un documento, aplica una función matemática sobre el documento dando como resultado un digesto que es encriptado utilizando su clave privada. Este resultado será remitido al receptor con el documento y la clave pública del firmante.

El receptor del documento puede verificar la firma digital aplicando otra función matemática utilizando el documento remitido, el digesto encriptado y la clave pública del firmante. Si el resultado es positivo, significa que el documento no ha sido modificado y que proviene del firmante. Si el resultado es negativo, significa que el documento ha sido alterado o que la firma no corresponde al firmante.

Por ese motivo la normativa nacional atribuye dos presunciones legales a favor de la firma digital

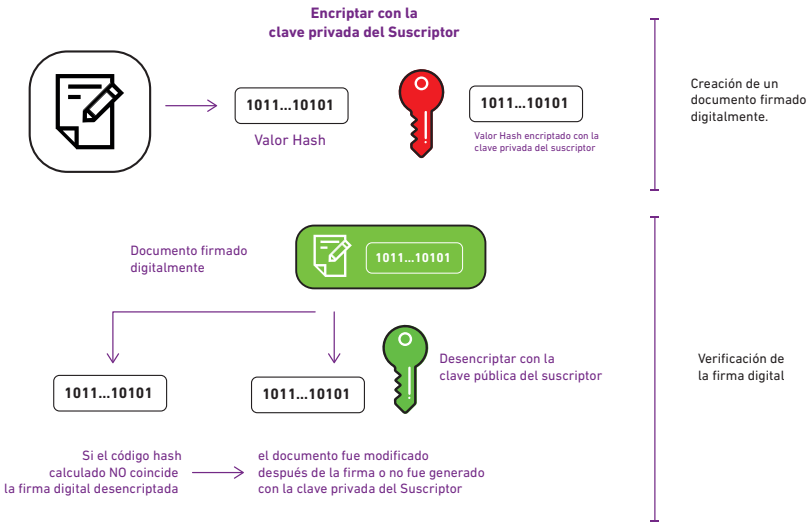
Creación y verificación de documento firmado digitalmente:

Autoría:

"Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma".
(artículo 7° de Ley N° 25.506)

Integridad:

"Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma" (art. 8° Ley N° 25.506)



Es muy importante destacar que todo el procedimiento necesario para firmar digitalmente un documento es realizado por el sistema o computadora. Las acciones que llevan adelante Suscriptor y receptor del documento son sumamente sencillas.

En el caso del Suscriptor (se entiende como tal al titular de una firma digital/firma electrónica), sólo debe conocer la contraseña del dispositivo criptográfico donde se encuentra alojado su certificado de clave pública.

Paso a paso de la Firma del Documento:

1° Calcular el hash del documento
2° Cifrar el hash con la clave privada del firmante
3° Enviar el documento al receptor, el hash cifrado y la clave pública del firmante

Paso a paso de la Validación de un documento

1° Calcular el hash del documento recibido
2° Descifrar el hash con la clave pública del firmante
3° Comparar ambos hashes

CERTIFICADOS DIGITALES

Ahora bien, cuando firmamos digitalmente un documento hay un tercer elemento esencial, además del par de claves: los certificados digitales.

Los certificados digitales son documentos electrónicos que contienen información sobre su titular (la identidad de una persona o entidad) y además expresan la clave pública que se utilizará para cifrar y descifrar mensajes.

Los certificados digitales se basan en el estándar X.509, que define el formato y los campos que debe tener un certificado. Entre estos campos se encuentran el nombre del Suscriptor, la fecha de emisión y caducidad del certificado, el algoritmo de cifrado utilizado, la firma de la autoridad de certificación y la clave pública del titular. En pocas palabras, este certificado digital nos permitirá vincular la clave pública (que se corresponde con una privada) con su titular o Suscriptor (persona física o entidad).

La normativa nacional refiere en el art. 14 de la Ley N° 25.506, que "Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular".

CERTIFICADOR LICENCIADO PROVINCIAL

El Certificador Licenciado es una tercera parte de confianza que expide certificados y cuenta con una licencia para ello, otorgada por el ente licenciante.

En nuestro caso, la Ley N° V-0591-2007 de firma digital reglamentada por Decreto N° 0428-MP-2008 modificado por Decreto N° 6011-MCyT-2018, el Instituto Firma Digital de San Luis, actúa como Certificador Licenciado Provincial. Las entidades emisoras de certificados están organizadas en una jerarquía de Autoridades Certificantes. En este sentido existe una Autoridad Certificante Raíz Provincial, que es administrada por el Ente Licenciante Provincial, a través de la que se emiten certificados digitales a las Autoridades Certificantes Subordinadas, administradas por los Certificadores Licenciados por la provincia.

Las Autoridades Certificantes son un componente esencial de la solución de PKI (public key infraestructure, por sus siglas en inglés). Realizan las siguientes tareas:

- ***Verifica la identidad de los solicitantes de certificados.***
- ***Emiten certificados de clave pública para los suscriptores***
- ***Gestionan la revocación de los certificados de clave pública de los suscriptores.***

La normativa provincial así como la nacional permiten que la tarea de validación sea realizada por una AUTORIDAD DE REGISTRO.

AUTORIDAD CERTIFICANTE

FDSL optó por una Jerarquía de Tres Niveles. Una Autoridad Certificante Raíz que se autoemite, y una Autoridad Certificante Intermedia, que emitirá los certificados a las Autoridades Certificantes Subordinadas. De este modo se logró una mayor seguridad toda vez que la primera siempre se encuentra fuera de línea.

La AC Raíz y la AC Intermedia son administradas por el Ente Licenciante Provincial.

JERARQUÍA DE AUTORIDADES CERTIFICANTES:

AC RAÍZ:

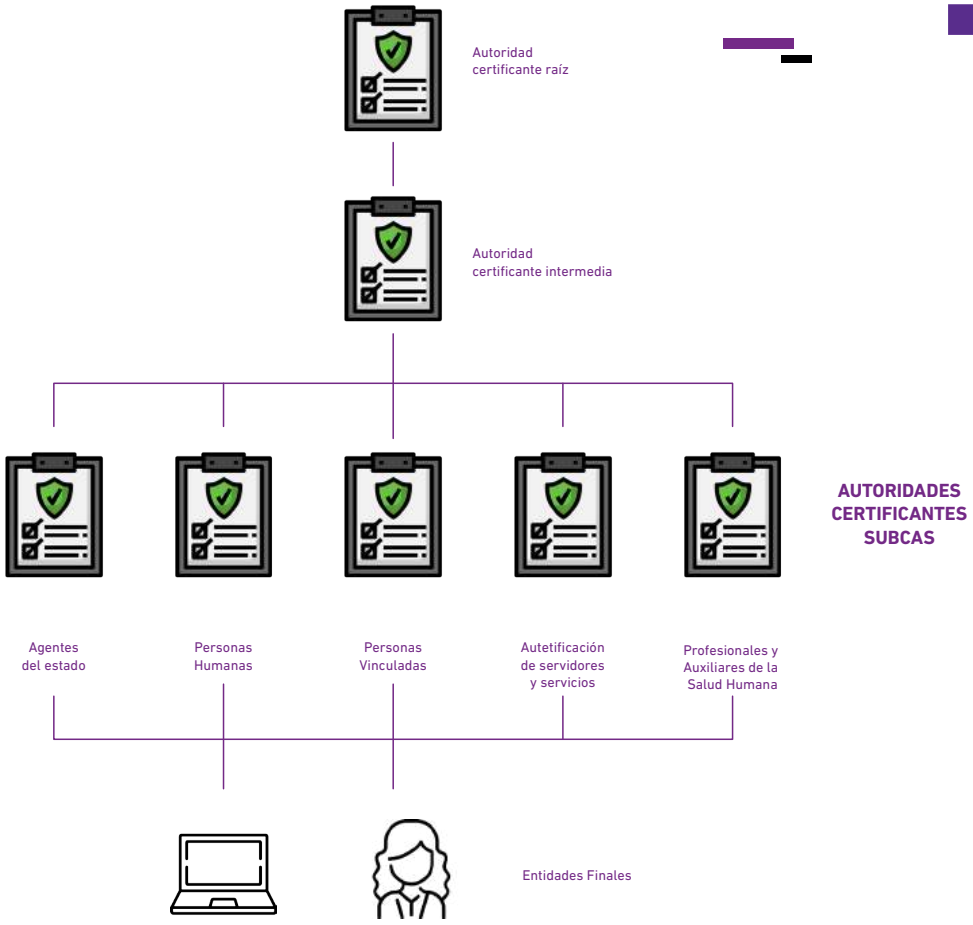
- AC superior en jerarquía.
- Punto de Confianza de todos los certificados.
- Auto emite su certificado.

AC INTERMEDIA

- Complementaria a la AC RAÍZ (existe por motivos de seguridad).
- Emite a las AC Subordinadas que la AC RAÍZ disponga.

AC SUBORDINADAS

- Deben ser aprobada por la AC RAÍZ.
- Corresponde a una Política de Certificación.
- Emite certificados a usuarios finales (Suscriptores)



Todas las Autoridades Certificantes se alojan en servidores especiales, que a su vez están ubicados en nuestra sala cofre cuyas características están detalladas en el Capítulo correspondiente.

3

IMPLEMENTACIÓN DE LA FIRMA DIGITAL EN SAN LUIS

IMPLEMENTACIÓN DE LA FIRMA DIGITAL EN SAN LUIS

En este sentido, en el año 2006 la Provincia encontró en la firma digital la herramienta que permitiría digitalizar su rol administrativo logrando una gestión ágil y transparente acercándose además a sus habitantes.

Para ello, fue necesario poseer la normativa que le diera respaldo.

En ese entonces, Argentina contaba con la Ley N° 25.506, de Firma Digital, que tácitamente modificaba la normativa de fondo otorgándole valor jurídico al documento electrónico, a la firma electrónica y a la firma digital. Además la Ley le asignaba a todos estos elementos un importante valor probatorio. Esta norma invitaba a las Provincias a adherir a su texto.

En ese marco San Luis dictó la Ley N° V-0591-2007 adhiriendo a Ley Nacional N° 25.506, en sus Capítulos I a IV, y en pleno ejercicio de su autonomía provincial determinó su ámbito de aplicación, su autoridad de aplicación, plazos de despapelización, pautas para su funcionamiento, el reconocimiento de certificadores licenciados provinciales, la constitución de autoridades de registro, la aplicación de un sistema de multas y sanciones, condiciones de confidencialidad, etc.

INFRAESTRUCTURA DE FIRMA DIGITAL DE SAN LUIS

San Luis tomó la decisión de crear su propia infraestructura de clave pública ya que en la provincia existía un escenario propicio para poner en funcionamiento en poco tiempo una Administración Digital: todas las dependencias del estado se encontraban conectadas a internet, se entregaban dispositivos electrónicos a diversos sectores de la sociedad y existían además facilidades para su adquisición. Todo ello, acompañado de proyectos de capacitación en el uso de herramientas digitales que estaban en total ejecución y que con los años se irían incrementando.

El hecho que a nivel nacional aún no existiera un Plan Digital, y especialmente, una Autoridad Certificante Raíz que emitiera certificados a sus Certificadores Licenciados confirmó la conveniencia de que la provincia ejecutara esta iniciativa de manera autónoma. Decisión, que años más tarde, diversas circunstancias confirmaron que era la más adecuada aunque lamentablemente hasta el día de la fecha Provincia y Nación no han logrado cruzar los Certificados de Clave Pública de sus correspondientes Autoridades Certificantes Raíz, lo que permitiría la interacción total de ambas infraestructuras. Es penoso mencionar que desde el año 2009 hasta la fecha de publicación de este libro este impedimento persiste porque cada solicitud formal de la Provincia fue extraviada en el Gobierno Nacional.

San Luis construyó su infraestructura de clave pública cumpliendo los estándares internacionales de tecnología dentro de su Data Center, y en el año 2019 renovó la totalidad de su equipamiento para robustecer su seguridad y comenzar a utilizar el algoritmo SHA-2.
En el año 2009 se emitió el certificado RAIZ de San Luis

y desde ese entonces hasta hoy, se continúa emitiendo firma digital al sector público y privado. Hasta el día de la fecha hemos emitido más de novecientos mil certificados de clave pública y la provincia basa gran parte de su estrategia de digitalización en el uso de firma digital.

En una primera etapa se promovió el uso de la firma digital en la órbita del Estado Provincial. El Gobierno adquirió un sistema de gestión de expedientes para ser utilizado en la administración central, se realizó una prueba piloto exitosa en la Universidad de La Punta, y en el transcurso del primer año se logró que fuera utilizado por el ciento por ciento de los Ministerios, Contaduría General, Fiscalía de Estado y el Tribunal de Cuentas.

Una de las estrategias que resultó vital para el éxito en la implementación fue que los organismos provinciales de control fueron de los primeros en utilizar el sistema y la firma digital, garantizando desde el inicio del proyecto su transparencia y agilidad en la gestión. Pero la medida más importante de todas fue la decisión y respaldo del entonces gobernador, Alberto Rodríguez Saá, en despapelizar el Estado.

Se estableció una fecha de quiebre a partir de la cual la totalidad de los expedientes serían generados en formato digital. Durante los dos primeros años de implementación coexistieron los expedientes que habían "nacido" en formato papel con los digitales, hasta que finalmente la totalidad de la administración pública trabajó digitalmente. Paralelamente, se licitó un sistema de gestión de expedientes para ser utilizado en el Poder Judicial de la Provincia de San Luis que permitiera la interacción de abogados, auxiliares y toda la ciudadanía con el servicio

de justicia y que tuvo como pilar fundamental la utilización de firma digital por parte de todos los participantes del proceso judicial (jueces, secretarios, abogados, peritos, ciudadanos).

Este sistema, en el Poder Judicial, se comenzó a implementar en el 2009 e incorporó la totalidad de la estructura judicial, es decir, Juzgados, Cámaras de Apelaciones, Superior Tribunal, Ministerios Pupilares, Ministerios Fiscales, Organismos auxiliares, Mediación, Cuerpo Forense, Contralor de Tasa y Contable, Secretaria Administrativa, inclusive Colegios Profesionales de Abogados y Peritos Judiciales. En ese período se mantuvo un expediente "doble" ya que coexistía el expediente papel (como cortesía) y los abogados podían presentar escritos por la web de manera voluntaria. En el año 2014 se creó el primer juzgado totalmente digital, y en este mismo año paulatinamente se volvió obligatorio para una de las tres Circunscripciones en las que se encuentra dividida la Justicia Provincial; luego se fueron incorporando los fueros de las restantes Circunscripciones.

Asimismo se optimizó la interacción electrónica entre el Poder Ejecutivo y el Poder Judicial, de manera que las comunicaciones entre ambos se realizan digitalmente y se continúan perfeccionando. Durante el año 2017, se ha digitalizado el sumario policial permitiendo desde entonces un contacto fluido en forma virtual entre el Poder Judicial y la Policía, dos espacios que trabajan constantemente unidos toda vez que la Policía actúa como auxiliar de la Justicia y una vez creado el sumario en sede policial, el mismo puede ser visualizado simultáneamente por el juez, creando un expediente digital en el Poder Judicial.

Desde el 2010 a la fecha el ahorro en papel en el Poder Ejecutivo representó más de un 85%.

Cantidad de Expedientes generados en la Administración Central desde el año 2010 hasta 2023: ***2.117.110***
Cantidad de actuaciones firmadas digitalmente en dichos expedientes: ***16.240.285***
De esta manera el proyecto evitó la emisión de 119.02 toneladas de CO2

La despapelización del sistema judicial propició el uso de la herramienta digital entre los particulares matriculados en diversos colegios profesionales.
Los primeros años supusieron un gran esfuerzo para lograr que el sector privado utilizara la herramienta, sin embargo quienes se animaron a utilizarla no demoraron en encontrar los beneficios que la firma digital brinda a la labor diaria.

Además de la despapelización del sector público provincial, San Luis se abocó a sumar al sector privado a esta iniciativa. Se provee firma digital a matriculados de varias profesiones tales como abogados, ingenieros, agrónomos, arquitectos, agrimensores, profesionales de ciencias económicas, martilleros, corredores públicos, profesionales y auxiliares de la salud humana. Para proveer firma digital a los profesionales, el Instituto FDSL constituye Autoridades de Registro en los Colegios Profesionales, ya que sin duda ellos están en mejores condiciones de verificar quién se encuentra matriculado y que la matrícula del colegiado se encuentra vigente. Asimismo, en el supuesto que fuera suspendida o cancelada, el Colegio tramita inmediatamente la revocación del certificado correspondiente al profesional involucrado.

San Luis incorporó a través de diferentes reparticiones la posibilidad de realizar presentaciones y trámites electrónicamente firmadas digitalmente, agilizando la tarea de los profesionales.

La emisión de firma digital a través de los Colegios Profesionales facilitó el orden y control inherente a esas entidades deontológicas, lo que redundó en beneficio para el Estado, los profesionales, los Colegios y los ciudadanos. Desde el año 2009 San Luis realiza sus mayores esfuerzos para incentivar el uso de la firma digital por parte de los ciudadanos particulares. En este sentido la Ley Provincial Nº V-0698-2009 creó la Cédula de Identidad Provincial Electrónica (CIPE) con la finalidad de contener en una misma cédula todos los datos necesarios para la identificación de la persona, tanto física como digitalmente, garantizando la protección de los datos personales de su titular. Esta tarjeta de identificación posee un dispositivo criptográfico donde al momento de tramitarla le es generado un certificado de firma digital que podrá utilizar para firmar documentos digitales. La Cédula de Identidad Provincial Electrónica (CIPE), comienza su emisión en el 2010. Su emisión es gratuita, rápida y ágil.

Para las personas con domicilio en municipios adheridos a la Ley CIPE/LC y de Tránsito Provincial, se incluye, en el mismo soporte (tarjeta inteligente), la licencia de conducir nacional (CIPE-LC). A partir del 2017 también se incluye en esta tarjeta identificatoria, los datos de los Certificados Únicos de Discapacidad (CUD) para quienes son beneficiarios del carnet de discapacidad y el pase libre para transporte público con la finalidad de facilitar el acceso a los beneficios que la legislación concede a aquellas personas con capacidades diferentes.

San Luis es el único Estado en el continente americano que distribuye un documento de estas características.

En marzo de 2017 se actualizó la CIPE a la nueva CIPE 3.0 con tecnología NFC (Near Field Communication) que permite a los habitantes de San Luis firmar digitalmente desde dispositivos móviles que posean la misma tecnología, facilitando la interacción entre personas, empresas y gobierno. De esta manera se busca simplificar la utilización de firma digital sin la necesidad de un lector. Durante 2017 en línea con la entrega de tabletas con tecnología NFC sumado a la emisión gratuita de CIPE 3.0 para todos los habitantes de San Luis, se actualizó el Portal Ciudadano de la Provincia de San Luis, denominado Portal Puntano, hacia una nueva versión que aproveche todas las potencialidades de la digitalización de la provincia. Esta nueva versión, Portal Puntano 3.0 (Aplicación Web y Aplicación para Móviles), incorpora una Guía de Trámites y permite la ejecución en línea de trámites contra el Gobierno Provincial y los Municipios de San Luis.

Ejemplo de ello constituye el trámite de "Denuncia en Defensa del Consumidor". Previo al lanzamiento de Portal Puntano 3.0, Defensa del Consumidor disponía de tres ubicaciones físicas en la Provincia donde receptar los reclamos de los consumidores, actualmente mediante Portal Puntano y la infraestructura digital de la Provincia que posibilita el Wifi gratuito en todo rincón de la geografía provincial, pueden realizar la denuncia correspondiente en toda la Provincia de San Luis, con solo contar con un dispositivo móvil con NFC, conectividad Wifi y CIPE 3.0.

Para generalizar el uso de la CIPE 3.0, se ha diseñado una app que permite enviar y recibir documentos para su firma. Poniendo el DNI de la persona que debe firmar el documento, su dirección de mail y adjuntando el archivo en PDF, se enviará el mismo para su firma.

La app que funcionará para dispositivos con sistema operativo Android con NFC, avisará al firmante que tiene un documento para su firma.

Apoyando la CIPE 3.0, y poniendo el password definida al momento de la emisión de la CIPE 3.0, el documento es firmado digitalmente, avisando al emisor que ya está disponible el documento firmado.

Asimismo San Luis cuenta con la plataforma de Comisaría Virtual, es un sitio web www.va.sanluis.gov.ar y una App, disponible para Android, que permite a todos los habitantes de San Luis realizar trámites policiales de manera online, a través de la firma digital.

Los trámites que pueden realizarse con la app de la Comisaría Virtual son:

Certificado de domicilio:

Este trámite permite obtener un certificado digital donde consta el domicilio del solicitante, para ser presentado ante el organismo que el solicitante declare.

Certificado de estadía:

certifica la presencia temporal del solicitante en algún lugar diferente al domicilio que consta en su documento de identidad. El solicitante debe estar en el lugar temporal al momento de realizar el pedido, para que el GPS del dispositivo registre la ubicación del mismo.

Certificado de supervivencia:

La Administración Nacional de la Seguridad Social (ANSES) exige que todos los jubilados y pensionados den fe de vida periódicamente ante la entidad bancaria o centro de pago en la que cobran sus haberes jubilatorios. Si no se realiza en el plazo establecido, la entidad suspende el pago del haber jubilatorio. Este trámite puede ser solicitado por un familiar, la policía deberá asistir al domicilio del jubilado o pensionado y verifica que se encuentra vivo, emitiendo el certificado firmado digitalmente.

Constancia de extravío:

En este trámite el solicitante describe los objetos extraviados y la policía da fe de los dichos del solicitante, no del extravío en sí.

Exposición ciudadana:

La exposición es la certificación policial de las manifestaciones de una persona, sobre un acontecimiento que no llega a ser delito, no dando inicio a una investigación penal.

Denuncia ciudadana:

a través de este acto se da noticia de la existencia de un posible delito ante la autoridad policial o judicial, dando inicio a una investigación penal

Certificado de antecedentes:

el certificado de antecedentes policiales y penales es un documento electrónico firmado digitalmente por la autoridad policial que certifica que el solicitante no tiene antecedentes o procesos penales pendientes.

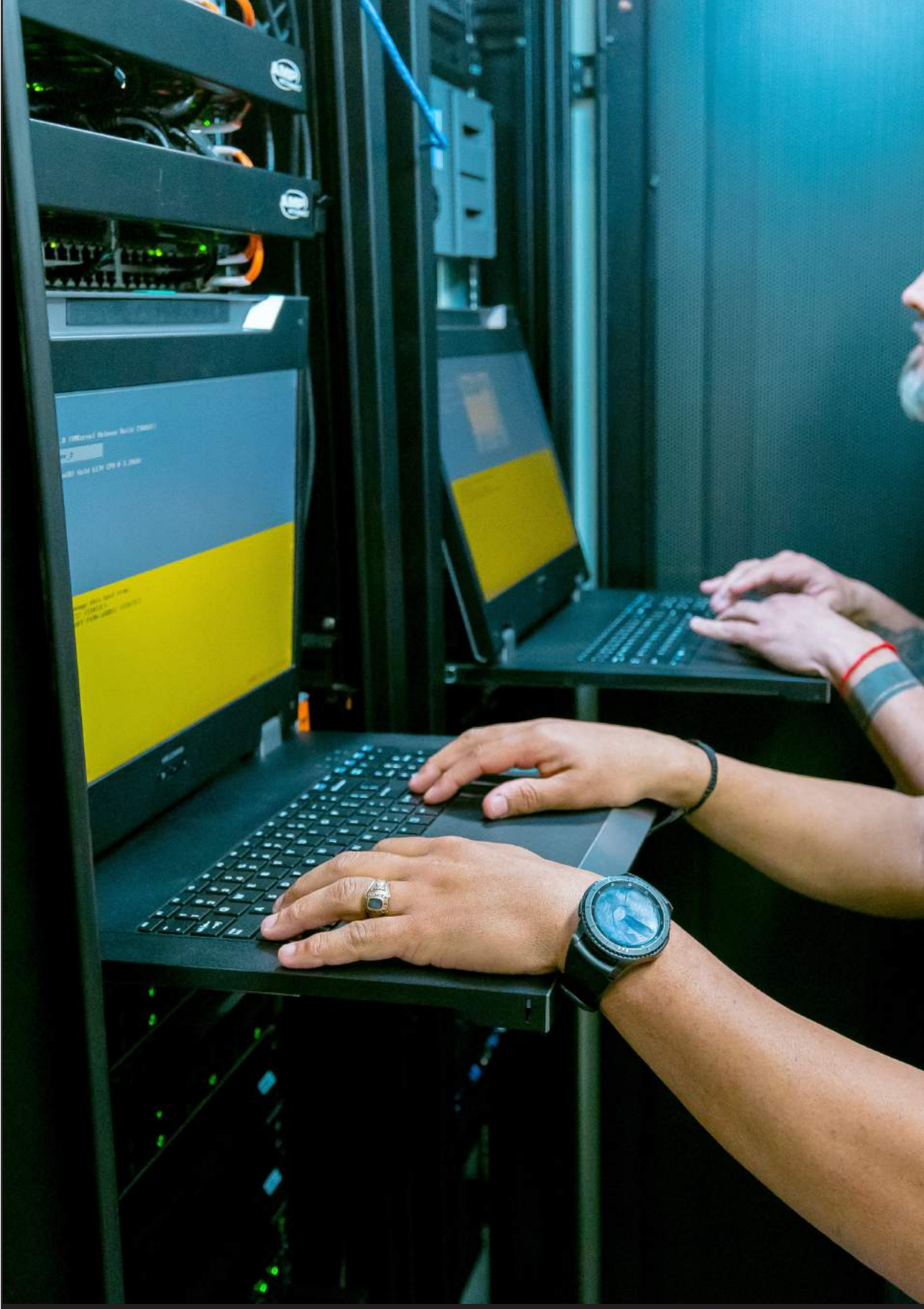
Alarma Puntana:

con este trámite se asigna/modifica el número del celular y el número de teléfono alternativo del usuario de la alarma puntana, este trámite tiene que ser firmado digitalmente.

El usuario de esta aplicación requiere tener un dispositivo móvil con tecnología NFC y la Cédula de Identidad Provincial Electrónica 3.0. o 4.0.

EMPRESAS

San Luis emite firma digital a los dependientes, representantes y apoderados de empresas quienes no sólo la utilizan en su interacción en el Estado sino también para su gestión interna.



4

POLÍTICAS DE CERTIFICACIÓN

OFF-WHITE
ISLEAN

POLÍTICAS DE CERTIFICACIÓN

La Política de Certificación es un documento legal que contiene las normas relativas al ciclo de vida de un certificado digital: requisitos de emisión, plazo de vigencia, usos, causales de revocación, responsabilidad de las partes, entre otros. De acuerdo con las cuales, se puede considerar que una firma digital es válida. Abarca desde la creación hasta la extinción de un certificado digital.

En San Luis existen 5 Políticas de Certificación vigentes:

- ***Firma Digital de Agentes del Estado.***
- ***Firma Digital para Personas Vinculadas.***
- ***Firma Digital para Profesionales y Auxiliares. de la Salud Humana***
- ***Firma Digital para Personas Humanas.***
- ***Servidores y Servicios.***

POLÍTICA DE CERTIFICACIÓN DE FIRMA DIGITAL PARA AGENTES DEL ESTADO

La Política de Certificación para Agentes del Estado permite que todos los agentes que desempeñan una tarea en el Estado Provincial, Municipal o incluso Nación, puedan tramitar esta firma digital, independientemente el tipo de relación que los vincule.

Esta fue la primera Política de Certificación en ponerse en funcionamiento y en virtud de la misma el Instituto de Firma Digital San Luis celebró convenios con cada Ministerio, Organismo Público, Municipios, etc., estableciendo en los mismos el mecanismo para acreditar quién estaría a cargo de validar que una persona se desempeña en ese Organismo. Por ejemplo, en el caso de la Universidad de La Punta en el convenio celebrado se dispuso que cada Secretario de la Institución debe extender una nota solicitando se expida el certificado de clave pública para los agentes que se desempeñan en su órbita. Y cuando un agente se desvincula o cambia el rol que desempeña en la Universidad, es el Secretario quien está facultado para solicitar la revocación del certificado sin perjuicio de la obligación del suscriptor.

Estos certificados le permiten al receptor del documento conocer información detallada el emisor como su nombre completo, documento nacional de identidad, el rol que desempeña en el organismo, y el detalle del suborganismo al que pertenece, en caso de corresponder. Se podría trazar un paralelismo entre los datos informados en un certificado con los contenidos en un sello del firmante.

LISTADO DE REPARTICIONES U ORGANISMO CON QUIEN SE HA CELEBRADO CONVENIO A FIN DE EMITIR FIRMA DIGITAL A SUS DEPENDIENTES

- Municipalidad de Balde
- Municipalidad de Batavia
- Municipalidad de Beazley
- Municipalidad de Buena Esperanza
- Municipalidad de Candelaria
- Municipalidad de Carpintería
- Municipalidad de Juana Koslay
- Municipalidad de Justo Daract
- Municipalidad de la Ciudad de La Punta
- Municipalidad de San Luis
- Municipalidad de Villa Mercedes
- Municipalidad de Comunidad Huarpe De Guanacache
- Municipalidad de Comunidad Pueblo Nación Ranquel
- Municipalidad de Concarán
- Municipalidad de Cortaderas
- Municipalidad de Desaguadero
- Municipalidad de El Trapiche
- Municipalidad de El Volcán
- Municipalidad de Estancia Grande
- Municipalidad de Fortín El Patria
- Municipalidad de Fortuna
- Municipalidad de Fraga
- Municipalidad de Juan Jorba
- Municipalidad de Juan Llerena
- Municipalidad de La Calera
- Municipalidad de La Carolina
- Municipalidad de La Punilla
- Municipalidad de La Toma
- Municipalidad de La Vertiente
- Municipalidad de Lafinur La Lomita
- Municipalidad de Las Aguadas - Rincón Del Carmen
- Municipalidad de Las Chacras
- Municipalidad Las Lagunas - Guzmán
- Municipalidad de Lavaisse
- Municipalidad de Los Manantiales
- Municipalidad de Los Molles
- Municipalidad de Lujan
- Municipalidad de Naschel
- Municipalidad de Navia
- Municipalidad de Nogolí
- Municipalidad de Nueva Galia
- Municipalidad de Papagayos
- Municipalidad de Paso Grande
- Municipalidad de Potrero De Los Funes

- Municipalidad de Quines
- Municipalidad de Renca
- Municipalidad de Saladillo
- Municipalidad de San Francisco del Monte de Oro
- Municipalidad de San Jerónimo
- Municipalidad de San José Del Morro
- Municipalidad de San Martín
- Municipalidad de San Pablo
- Municipalidad de Santa Rosa del Conlara
- Municipalidad de Talita
- Municipalidad de Tilisarao
- Municipalidad de Unión
- Municipalidad de Villa de La Quebrada
- Municipalidad de Villa de Merlo
- Municipalidad de Villa de Praga
- Municipalidad de Villa Larca
- Municipalidad de Zanjitas
- Municipalidad de Leandro N. Alem
- Municipalidad de Villa Del Carmen

En el marco de esta Política de Certificación FDSL cuenta con 13 Autoridades de Registros y 36 Oficiales de Registro además del propio Instituto.

- Cámara de Senadores de San Luis
- CPO San Luis
- CPO Unidad Regional II - VM
- CPO Unidad Regional III - Concarán
- FDSL CIPE
- Honorable Tribunal de Cuentas
- Ministerio de Educación de San Luis
- Municipalidad de Villa Mercedes
- Universidad de Los Comechingones
- Poder Judicial Concarán
- Poder Judicial San Luis
- Poder Judicial Santa Rosa
- Poder Judicial Villa Mercedes

POLÍTICA DE CERTIFICACIÓN DE FIRMA DIGITAL PARA PERSONAS VINCULADAS

La Política de Certificación para Personas Vinculadas, permite emitir certificados digitales a todas las personas físicas que deseen firmar describiendo o detallando su vínculo, relación o dependencia con una persona jurídica, pública o privada.

En el marco de esta Política el Instituto celebró convenios con la mayoría de los Colegios Profesionales de la provincia o entidades deontológicas de San Luis.

LISTADO DE COLEGIOS PROFESIONALES CON QUIENES SE HA CELEBRADO CONVENIO PARA EMITIR FIRMA DIGITAL A SUS MATRICULADOS

- Colegio de Abogados y Procuradores de Concarán
- Colegio de Abogados y Procuradores de la Ciudad de San Luis
- Colegio de Abogados y Procuradores de la Ciudad de Villa Mercedes
- Colegio de Escribanos de la Provincia de San Luis
- Colegio de Ingenieros Agrónomos y Profesiones Afines
- Colegio de Ingenieros y Técnicos de la Ingeniería
- Consejo Profesional de Ciencias Económicas San Luis
- Consejo Profesional de Ciencias Económicas Villa Mercedes
- Colegio de Agrimensura
- Colegio de Arquitectos
- Colegio de Geología de la Provincia de San Luis

- Colegio de Magistrados y Funcionarios Judiciales de San Luis
- Colegio de Martilleros y Corredores Públicos
- Colegio de Profesionales de Higiene y Seguridad en el Trabajo de la Provincia de San Luis
- Registro de Profesionales Matriculados como Responsables Técnicos de Residuos Peligrosos – SEMAP
- Registro Único de Consultores en Estudios de Impacto Ambiental – SEMAP
- Secretaría Administrativa del Superior Tribunal de Justicia de San Luis (registra peritos y mediadores)

El primero de los Colegios Profesionales en sumarse al uso de firma digital en San Luis, fue el Colegio de Abogados de la Ciudad de San Luis. Se celebró un convenio en el que se designó la persona encargada de acreditar el vínculo del solicitante del certificado con el Colegio Profesional de manera tal que es éste quien da fé que una persona se encuentra matriculada y que esa matrícula está vigente. Si la matrícula es suspendida o cancelada, el Colegio Profesional tiene la obligación de notificar esa circunstancia al Instituto para que éste proceda a revocar el certificado digital.

En los certificados digitales de los profesionales matriculados se puede observar además de sus datos personales (nombre completo y número de documento), los datos del Colegio Profesional, profesión bajo la cual se encuentra matriculado el suscriptor, y de corresponder, número de matrícula.

En virtud de esta Política de Certificación también se emiten certificados a personas que desean firmar digitalmente en su rol de dependiente, representante o miembro de una persona jurídica, como podría ser el caso del apoderado de una Sociedad Anónima por ejemplo. En estos casos, la Persona Jurídica debe acreditar su existencia con la documentación pertinente, solicitar la emisión del certificado con una nota de su representante legal y luego el Sucriptor, debe acreditar su identidad.

Cuando la empresa solicita certificados digitales para muchos de sus dependientes, el Instituto celebra un convenio designando al responsable de solicitar la emisión de las firmas. Generalmente se trata del responsable de Recursos Humanos de manera tal de agilizar el trámite de emisión.

En la actualidad son 15 las Autoridades de Registro constituídas a fin de emitir estas firmas firmas digitales y 49 los Oficiales de Registro en función.

Colegio de Abogados y Procuradores Concarán
Colegio de Abogados y Procuradores San Luis
Colegio de Abogados y Procuradores Villa Mercedes
Colegio de Escribanos
Colegio de Ingenieros Agrónomos y Profesiones Afines
Colegio de Ingenieros y Técnicos de la Ingeniería
Consejo Profesional de Ciencias Económicas de San Luis
Consejo Profesional de Ciencias Económicas de Villa Mercedes
Poder Judicial de Concarán
Poder Judicial de San Luis
Poder Judicial de Santa Rosa del Conlara
Poder Judicial de Villa Mercedes
Camuzzi Gas del Sur
Camuzzi Gas Pampeana
Gerencia CIPE 4.0
INTI

POLÍTICA DE CERTIFICACIÓN DE FIRMA DIGITAL PARA PROFESIONALES Y AUXILIARES DE LA SALUD

La Política de Certificación para Profesionales y Auxiliares de la Salud enmarca la emisión de firma digital a todas las personas que ejercen alguna profesión o actividad vinculada con la salud en la provincia de San Luis, comprendidas en la Ley N° XIV-0361-2004. Se utiliza especialmente para todas aquellas iniciativas vinculadas con Historia Clínica Digital. Los certificados emitidos detallan los datos personales del Suscriptor (nombre completo y número de documento), los datos del Colegio Profesional, profesión bajo la cual se encuentra matriculado el suscriptor y el número de matrícula.

LISTADO DE COLEGIOS PROFESIONALES O ENTIDADES DEONTOLÓGICAS CON QUIENES SE HA CELEBRADO CONVENIO PARA EMITIR FIRMA DIGITAL A SUS MATRICULADOS

- Ministerio de Salud de San Luis - Subprograma Asuntos Profesionales
- Colegio de Farmacéuticos de San Luis
- Colegio de Profesionales de Servicio Social de San Luis
- Colegio de Psicólogos de San Luis

En la actualidad hay 2 Autoridades de Registro constituídas a fin de emitir estas firmas firmas digitales y 20 los Oficiales de Registro en función.

- ***Asuntos Profesionales Ministerio de Salud***
- ***Gobierno Digital***

POLÍTICA DE CERTIFICACIÓN DE FIRMA DIGITAL PARA PERSONAS HUMANAS

La Política de Certificación para Personas Humanas permite a toda persona física tramitar una firma acreditando su identidad.

Toda persona titular de una Cédula de Identidad Provincial Electrónica (CIPE) posee esta firma digital que le permite realizar diversos trámites.

POLÍTICA DE CERTIFICACIÓN DE SERVIDORES Y SERVICIOS

La Política de Certificación de Servidores y Servicios permite la emisión de certificados que son utilizados a los fines de autenticar la identidad de un servidor y establecer luego un canal de transmisión seguro entre el servidor y el usuario del servicio.

Los certificados de sellado de tiempo, se utilizan a fin de garantizar la fecha y hora de las transacciones y el no repudio.

Suman un total de 50 las Autoridades de Registro constituídas en cada uno de los Centros de Emisión CIPE, siendo 150 los Oficiales de Registro en funciones.

TRÁMITE PARA LA EMISIÓN DE FIRMA DIGITAL

La firma digital en San Luis necesariamente debe tramitarse de manera presencial para que el Instituto pueda verificar la identidad del Solicitante quien se presentará ante sus Oficinas, o ante alguna Autoridad de Registro, con su documento nacional de identidad o cédula de identidad provincial electrónica y un dispositivo criptográfico.

Luego de verificar la identidad del Solicitante, el Instituto validará que aquel cumpla el resto de los requisitos según el certificado que esté tramitando. Por ejemplo, si se trata de un profesional, el Instituto corroborará que el Colegio correspondiente haya remitido nota acreditando que se encuentra debidamente matriculado; si se trata de un dependiente de un Ministerio, que el Ministerio donde aquel se desempeña lo solicitó por nota dando fe que allí se desempeña; etc.

Cumplido ello, se procederá a generar el certificado en un dispositivo criptográfico que el propio suscriptor debe poseer y cuya contraseña no debe jamás compartir con nadie, ya que esa contraseña es la “llave de acceso” que permitirá a nuestra computadora utilizar la clave privada de su certificado digital para firmar digitalmente.

DISPOSITIVOS CRIPTOGRÁFICOS

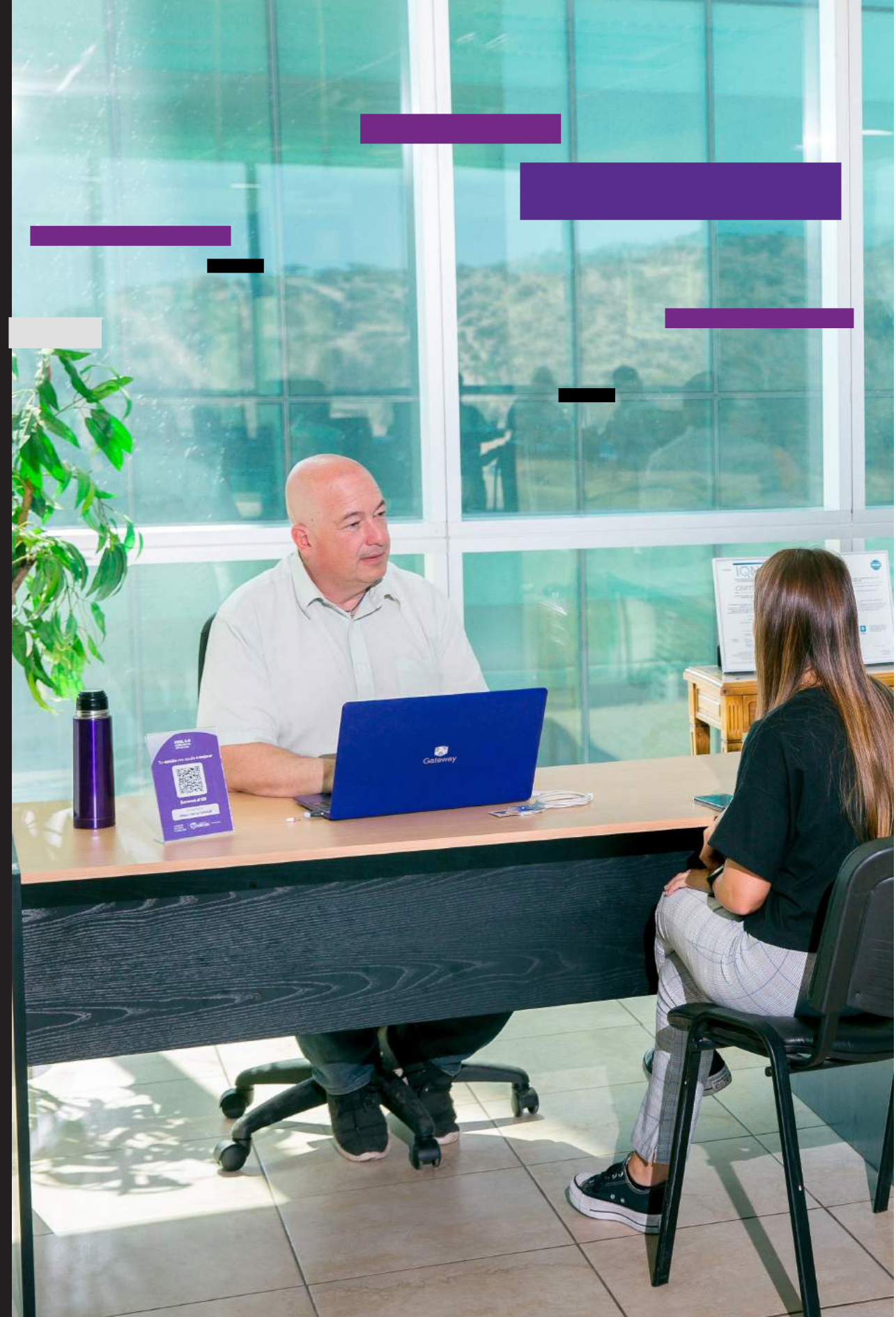
El Instituto Firma Digital San Luis sólo emite certificados de clave pública en dispositivos criptográficos aprobados por el NIST (National Institute of Standard and Technology), quien establece los requerimientos de seguridad que deben cumplir los módulos criptográficos utilizados para la protección de datos sensibles.

Únicamente se acepta el uso de dispositivos criptográficos que cumplen con FIPS 140 nivel 2 o superior, y se hayan incluídos en el sistema de emisión de FDSL.

TRÁMITE PARA LA REVOCACIÓN DE FIRMA DIGITAL

Los Suscriptores pueden tramitar la revocación de su certificado de firma digital de manera remota, solicitándolo a través de la página web de FDSL, vía correo electrónico firmado digitalmente o de manera presencial.

En cada Política de Certificación está prevista la nómina de personas que además del propio titular están facultados, o incluso en algunos casos están obligados, a solicitar la revocación de un certificado. Las causales son de lo más variadas y amplias respetando lo previsto en la normativa nacional y buscando garantizar la seguridad del Suscriptor.


Gateway

AUTORIDADES DE REGISTRO

La normativa permite que el trámite de emisión se realice ante el propio Instituto o lo haga a través de una Autoridad de Registro. Éstas funcionan como intermediarias entre el solicitante y la Autoridad Certificante del Instituto.

El Instituto constituye Autoridades de Registro a través de la celebración de convenios con diversos organismos, como puede ser un Colegio Profesional. Actualmente FDSL posee constituidas las Autoridades de Registro Remotas detalladas en el Capítulo correspondiente.

Los responsables de las Autoridades de Registro, denominados Oficiales de Registro, se encuentran específicamente designados en dichos convenios, son capacitados por FDSL, se les otorga acceso al sistema FDSL y se les brinda un servicio de Mesa de Ayuda para asistirlos en cualquier dificultad o contratiempo que pudieran tener en los procesos de emisión y revocación, y son auditados periódicamente. Los Responsables de las Autoridades de Registro desempeñan un rol fundamental en este proceso de despapelización, no sólo por su intervención al emitir y revocar certificados de clave pública sino también porque han adoptado un rol casi evangelizador fomentando la digitalización y colaborando con el Suscriptor en sortear dudas e incluso inconvenientes.

El compromiso de las Autoridades de Registro sumado al trabajo minucioso de las auditorías realizadas por FDSL dieron como resultado un sistema administrativo robusto que respalda y garantiza nuestra firma digital.

5

RÉGIMEN DE AUDITORÍAS

OBJETIVOS

El objetivo de las auditorias, se centra en analizar y verificar el cumplimiento de los requisitos establecidos, es decir verificar que el proceso de emisión de certificados de firma digital se cumpla efectivamente, y así evitar posibles desvíos, y de esta manera incrementar la eficiencia operativa. Por lo tanto mediante las auditorías se analiza el desempeño de los Oficiales de Registro quienes son los responsables de emitir los certificados de firma digital. A través de las auditorías, comprobamos que se estén llevando a cabo debidamente sus funciones, y cuando es necesario, se toma las medidas correctivas correspondientes. Las auditorías nos permiten llevar a cabo un seguimiento detallado, son precisas para detectar cualquier desviación y de esta manera poder subsanarlas de forma rápida y eficaz. Cuando se llevan a cabo las auditorías, van encaminadas hacia el cumplimiento de los siguientes puntos:

- ***Evaluar la confiabilidad y calidad de los sistemas utilizados; la integridad, confidencialidad y disponibilidad de los datos.***

- ***Evaluar el cumplimiento de las especificaciones de la Política de Certificación, Manual de Procedimientos, Política de Privacidad.***

- ***Evaluar los procedimientos y métodos de emisión, renovación y revocación del certificado de clave pública.***
- ***Identificar áreas potenciales de mejoras en el proceso de emisión.***

- ***Verificar la corrección de los hallazgos detectados en las auditorías anteriores y verificación de los procedimientos de las nuevas emisiones.***

PERIODICIDAD DE LAS AUDITORÍAS DE FIRMA DIGITAL

Las Auditorías de Firma Digital se planifican a inicio de año, su periodicidad se ve plasmada en el Plan de Auditoría Interna (PAI). El sistema de FDSL cuenta con un Módulo destinado específicamente a Auditorías, al que todos los Oficiales de Registro tienen acceso. De este modo los Oficiales quedan notificados de las futuras auditorías a realizarse a lo largo del año. El Plan de Auditorias se encuentra sujeto a modificaciones, si así lo requiere el organismo auditado, es decir por el mismo medio que se notificó, será el mismo que se utilice para su reprogramación.

EJECUCIÓN DE LAS AUDITORÍAS

Las Auditorías se ejecutan en formato digital a través del sistema de FDSL, verificando la documentación de respaldo, tomando como referencia la Política de Certificación de FDSL por la cual se emitió el certificado, ya que los requisitos varían según la política. Una vez llevada a cabo la auditoría en formato digital, se procede a realizarla de manera presencial. En donde los auditores se hacen presentes en los organismos a auditar.

Auditorías Digitales: Inicialmente las auditorías se realizaban sólo presencialmente y luego se incorporaron las digitales ya que se observó que lograban optimizar el sistema en general. En las digitales se auditan por medio del sistema de FDSL el ciento por ciento de las emisiones y revocaciones realizadas por los organismos.

Las auditorías se realizan con un día de anticipación a la fecha de las auditorías presenciales que es notificada en el plan de auditorías. De esta manera nos permite tomar conocimiento de los posibles hallazgos; si los hubiera, posibilitando informarlos al momento de realizar la auditoría presencial. Llevándolas a cabo de esta manera, aumentamos la eficacia, ya que en el momento en que se realice la auditoría presencial, el auditor ya cuenta con las evidencias y puede informarlas de forma presencial al responsable del organismo, logrando tener una comunicación favorable entre el auditor y auditado, y realizando de este modo una capacitación continua en relación a los desvíos y su solución, como también al proceso en general.

Auditorías Presenciales: Para el desarrollo de las auditorías que se llevan a cabo de forma presencial, en el organismo a auditar donde se encuentra constituida la Autoridad de Registro, se analiza la documentación en formato físico que consiste en un único documento firmado en formato papel por el solicitante de firma digital y por el responsable de la Autoridad de Registro: el Acuerdo con Suscriptores. Cabe destacar que el mencionado documento es el único que FDSL conserva en soporte físico, como también el principal documento que valida la conformidad de su suscriptor y/o solicitante de firma digital.

Es dable señalar que el objetivo principal de las auditorías es el de determinar el grado de cumplimiento de los criterios a auditar.

INFORMES DE AUDITORÍAS

Concluida cada auditoría el equipo de Auditores de FDSL confecciona el correspondiente Informe consignando los hallazgos surgidos, los desvíos (observaciones – no conformidades), las sugerencias y/o recomendaciones. Este documento es de gran utilidad para tomar decisiones relacionadas a los hallazgos detectados.

Los Informes son notificados al organismo auditado. Asimismo son resguardados en el módulo de auditorías del sistema de FDSL, suscriptos digitalmente por la Coordinadora de Auditorías de FDSL para garantizar que no puedan sufrir alteración alguna.

HALLAZGOS DE AUDITORÍAS

La sección más trascendente del Informe de Auditoría es la denominada “Hallazgos”, en dónde se narra de manera explicativa y lógica los hechos detectados como desvíos, errores, debilidades y/o fortalezas.

Todo organismo debe realizar un tratamiento específico para cada hallazgo surgido en un plazo de treinta días de notificado.

El módulo de auditorías con el que cuenta FDSL le permite al equipo auditor monitorear el avance del tratamiento de cada hallazgo.

ARCHIVOLOGÍA Y DISPOSICIÓN FINAL

FDSL cuenta con un archivo propio al que sólo accede personal del Instituto luego de pasar varios accesos de seguridad. La finalidad de este archivo es conservar la documentación que respalda cada emisión de certificados.

Es decir, los Acuerdos con Suscriptores, que son documentos en formato físico que validan la conformidad de los suscriptores y/o solicitantes de firma digital. Asimismo se lleva un control de la totalidad de los legajos que se encuentran en digital en el sistema de FDSL.

De esta manera FDSL posee el control de la documentación física ante posibles requerimientos administrativos o judiciales. Los mismos se encuentran resguardados de forma segura, cada legajo se encuentra en su caja, cuerpo, estante y estantería correspondiente.

SISTEMA DE GESTIÓN DE CALIDAD SGC

En el año 2017 el Instituto comenzó a implementar un Sistema de Gestión de Calidad definiendo los elementos claves del sistema y estableciendo el soporte documental, asegurándose de manera consistente la mejora del desempeño y la eficacia de la organización, a partir de la planificación, control y mejora de sus procesos, garantizando el cumplimiento de los requisitos del producto/servicio, la satisfacción de los clientes, y la mejora continua.

En el mismo año el Instituto logró la certificación internacional de las Normas ISO 9001:2015, cumpliendo con los estándares internacionales de la norma, cuyo alcance es:

"Diseño y desarrollo, promoción, planificación, realización, control, asistencia y soporte al usuario, del servicio "Firma Digital 3.0". Administración y control del ciclo de vida del certificado de firma digital: desde el alta del organismo, la capacitación de los responsables de la operatoria, la solicitud de emisión de certificados de firma digital, pasando por validación de la identidad, y efectiva generación y descarga del certificado digital hasta su revocación."

Una vez certificado bajo la norma ISO 9001:2015 el Instituto se encuentra más cerca de los requisitos de sus clientes y suministra mayor satisfacción a los mismos, permitiendo que estén seguros de que recibirán el servicio adecuado.

En la actualidad mantenemos la certificación y continuaremos haciéndolo para seguir proporcionando un servicio de calidad a todos nuestros usuarios.

REGISTRO DE FORTALEZAS DE FIRMA DIGITAL

La certificación de normas de calidad por parte del Instituto FDSL favoreció su crecimiento y que se afianzara el uso de la firma digital en la provincia ya que a medida que pasaba el tiempo se perfeccionaba el sistema, se robustecía la infraestructura tecnológica y se generaban nuevas herramientas. Ello se ve reflejado en cada uno de los Informes de Auditoría Externa que señalaron en reiteradas oportunidades fortalezas:

Registro de Fortalezas de Firma Digital

Auditoría Externa del 22/11/18: Comprensión de la Organización y de su contexto/ Necesidades y expectativas de las partes Interesadas. Acciones para abordar los riesgos y las oportunidades: Es de destacar el modo en que la Organización, a través de su Conducción Estratégica/ Aplicación eficaz de los lineamientos/requisitos de referencia, se asegura el logro de los resultados previstos para su SGC.

Liderazgo y compromiso: *Se destaca como fortaleza el "Liderazgo y compromiso" para con el SGC., evidenciado a través de Nivel de Gestión/ Inversiones/ Mejoras logradas desde la última Auditoría.*

Enfoque al Cliente: *Se destaca como atributo del SGC., el Enfoque al Cliente. Evidenciado a través de Nivel de Servicio-Control de las Salidas No Conformes/Satisfacción Destinatarios.*

Personas: *Se destaca la competencia y el compromiso del personal en relación a su proceso. Evidenciado a través de Nivel de desempeño/Objetivos-Indicadores relacionados.*

Fortalezas

Situaciones y atributos del sistema de gestión destacables por su buen funcionamiento y su valor con respecto al desempeño general del sistema.

Norma(s) de referencia					Requisito de la norma	Redacción de la fortaleza
ISO 9001	ISO 14001	OHSAS 18001	ISO 45001	Otra:		
X					4.1/4.2-6.1	**Comprensión de la Organización y de su contexto/ Necesidades y expectativas de las partes Interesadas- Acciones para abordar los riesgos y las oportunidades** Es de destacar el modo en que la Organización, a través de su Conducción Estratégica/Aplicación eficaz de los lineamientos/requisitos de referencia, se asegura el logro de los resultados previstos para su SGC.
X					5.1	**Liderazgo y compromiso** Se destaca como fortaleza el "Liderazgo y compromiso" para con el SGC., evidenciado a través de Nivel de Gestión/ Inversiones/ Mejoras logradas desde la última Auditoría.
X					5.1.2	**Enfoque al Cliente** Se destaca como atributo del SGC., el Enfoque al Cliente. Evidenciado a través de Nivel de Servicio-Control de las Salidas No Conformes/Satisfacción Destinatarios.
X					7.1.2	**Personas** Se destaca la competencia y el compromiso del personal en relación a su proceso. Evidenciado a través de Nivel de desempeño/Objetivos-Indicadores relacionados.

Infraestructura: Se considera una fortaleza de la organización, la determinación y mantenimiento de la infraestructura necesaria para la operación de sus procesos evidenciado en: la metodología utilizada para realizar el resguardo de la información y las pruebas periódicas de restauración. La metodología de validación de los cambios del sistema informático a través del ambiente de test. El sistema de monitoreo de los sensores y el sistema de detección y extinción de incendios de Sala Cofre.

Toma de conciencia: Se destaca el compromiso de todo el personal entrevistado evidenciado en el reconocimiento de la importancia de su contribución a la eficacia y mejora del desempeño del sistema de gestión de la calidad.

Fortalezas

Situaciones y atributos del sistema de gestión destacables por su buen funcionamiento y su valor con respecto al desempeño general del sistema.

Norma(s) de referencia					Requisito de la norma	Redacción de la fortaleza
ISO 9001	ISO 14001	OHSAS 18001	ISO 45001	Otra:		
X					7.1.3	**Infraestructura** Se considera una fortaleza de la organización, la determinación y mantenimiento de la infraestructura necesaria para la operación de sus procesos evidenciado en: - la metodología utilizada para realizar el resguardo de la información y las pruebas periódicas de restauración. - la metodología de validación de los cambios del sistema informático a través del ambiente de test. - el sistema de monitoreo de los sensores y el sistema de detección y extinción de incendios de Sala Cofre
X					7.3	**Toma de conciencia** Se destaca el compromiso de todo el personal entrevistado evidenciado en el reconocimiento de la importancia de su contribución a la eficacia y mejora del desempeño del sistema de gestión de la calidad.

Auditoría Externa 02-12-2020

Se pudo evidenciar como una fortaleza de la organización la infraestructura informática alcanzada para dar servicio a los usuarios, la cual permite escalar en el tiempo y absorber a más usuarios atendidos en el futuro.

Fortalezas

Situaciones y atributos del sistema de gestión destacables por su buen funcionamiento y su valor con respecto al desempeño general del sistema.

Norma(s) de referencia					Requisito de la norma	Redacción de la fortaleza
ISO 9001	ISO 14001	OHSAS 18001	ISO 45001	ISO 29.990		
X					7.1.3	Se pudo evidenciar como una fortaleza de la organización la infraestructura informática alcanzada para dar servicio a los usuarios, la cual permite escalar en el tiempo y absorber a más usuarios atendidos en el futuro.

Auditoría Externa 07-12-2021

Se pudo identificar como una fortaleza de la organización el nivel de excelencia alcanzado y la constante innovación en los procesos de trabajo.
Se pudo identificar como una fortaleza de la organización los cambios realizados para proporcionar y mejorar la infraestructura necesaria para la operación de sus procesos y lograr la conformidad de los productos y servicios.

Fortaleza

La fortaleza (FO) es una situación o atributo del sistema de gestión destacable por su buen funcionamiento y su valor con respecto al desempeño general del sistema.

FO	Norma de referencia					Req. de la norma	Redacción del hallazgo
	IRAM-ISO 9001	IRAM-ISO 14001	OHSAS 18001	IRAM-ISO 45001	Otra:		
F1	X					5.1	Se pudo identificar como una fortaleza de la organización el nivel de excelencia alcanzado y la constante innovación en los procesos de trabajo.
F2	X					7.1	Se pudo identificar como una fortaleza de la organización los cambio realizado para proporcionar y mejorar la infraestructura necesaria para la operación de sus procesos y lograr la conformidad de los productos y servicios.

Auditoría Externa 21-06-2022

Se identificó como una fortaleza de la organización el trabajo realizado de promoción sobre el uso de firma digital en las diferentes dependencias de gobierno o privadas, el cual permite múltiple beneficios para los subscriptores al sistema.

Se pudo identificar como una fortaleza de la organización la disponibilidad de los sistemas de Firma Digital para todos los suscriptores, el cual ha sido demostrado con los indicadores de seguimiento con un alto nivel de desempeño a lo largo del periodo evaluado.

Fortaleza

La fortaleza (FO) es una situación o atributo del sistema de gestión destacable por su buen funcionamiento y su valor con respecto al desempeño general del sistema.

FO	Norma de referencia					Req. de la norma	Redacción del hallazgo
	IRAM-ISO 9001	IRAM-ISO 14001	IRAM-ISO 45001	IRAM-ISO 50001	Otra:		
FO 1	X					**8.2.1**	Se identificó como una fortaleza de la organización el trabajo realizado de promoción sobre el uso de firma digital en las diferentes dependencias de gobierno o privadas, el cual permite múltiple beneficios para los subscriptores al sistema.
FO 2	X					**9.1**	Se pudo identificar como una fortaleza de la organización la disponibilidad de los sistemas de Firma Digital para todos los subscriptores, el cual ha sido demostrado con los indicadores de seguimiento con un alto nivel de desempeño a lo largo del periodo evaluado.

CIPE 4.0
GOBIERNO DE SAN LUIS
Nº: 16.133.040
Observaciones
CÉDULA DE IDENTIDAD PROVINCIAL ELECTRÓN
Viuda de Soldados de la Brigada Heroica en el
del Derecho de Inclusión Social, según Ley N°
2017.

6

INFRAESTRUCTURA TECNOLÓGICA DE LA FIRMA DIGITAL DE SAN LUIS

FDSL 4.0

INFRAESTRUCTURA TECNOLÓGICA DE LA FIRMA DIGITAL DE SAN LUIS

La infraestructura tecnológica de la firma digital de San Luis es el conjunto de componentes necesarios para el funcionamiento y la gestión de los servicios empresariales de Tecnologías de la Información (TI) y entornos de TI. Estos componentes incluyen hardware, software, instalaciones y redes. Y cómo cada uno de ellos contribuye al funcionamiento general del FDSL.

El camino tecnológico tuvo sus inicios a través de la ***Licitación Pública N° 07/2008 "ADQUISICIÓN DEL DISEÑO E IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI), DISPOSITIVOS CRIPTOGRÁFICOS, SALA COFRE, SOFTWARE y HARDWARE PARA FIRMA DIGITAL"*** la cual tenía como finalidad establecer una infraestructura de clave pública que permitiera crear las condiciones de un uso confiable del documento suscripto digitalmente.

a. Construir la infraestructura establecida, tanto en obra civil necesaria, sala cofre, software y hardware de servidores y criptográfico, formación de recursos humanos y procedimientos de acuerdo a la normativa provincial y nacional.

b. Permitir el proceso de archivo y despapelización y generar las condiciones para el desarrollo del comercio electrónico.

c. Proveer el software y procesos para los servicios de emisión, revocación y administración de certificados, auditoría, y gestión de los mismos a fin de permitir la firma digital en las diferentes transacciones que se realizan diariamente en los organismos dependientes de los Poderes Ejecutivo, Legislativo y Judicial de la Provincia

de San Luis, como así también el de la comunidad toda.
d. Introducir al usuario en una Internet útil que tenga impacto en su vida real.

e. Aumentar la productividad de los organismos de gobierno, y los de la ciudadanía, a optimizar el manejo de la información y reducir los costos de almacenamiento y de traslado de papel (despapelización).
f. Realzar el uso de los servicios aportados por la Autopista de la Información.

g. Promover el perfeccionamiento de la organización y el adecuado funcionamiento de la Administración Pública Provincial. Así como el fomento y desarrollo del comercio celebrado con el empleo de las nuevas tecnologías de la información y las comunicaciones.

h. Permitir obtener los beneficios que la Ley Nacional N° 25.506 da al asimilar el documento digital al documento en papel, reconociendo validez y eficacia jurídica.

i. Brindar un marco normativo que favorezca el empleo y difusión de la transferencia electrónica de información y el uso de la firma digital en todos los organismos públicos, en el ámbito de los tres poderes de la Provincia y en el ámbito de los negocios privados.

j. Permitir probar inequívocamente que una persona firmó un documento digital y que dicho documento no fue alterado desde el momento de su firma, siempre que su implementación se ajuste a los procedimientos preestablecidos.

k. Implementar la firma digital en los sistemas de expedientes. Emitiendo los certificados para todos los usuarios involucrados utilizando dispositivos criptográficos estándar y biométricos, según sea la necesidad.

SALA COFRE

FDSL cuenta con un Ambiente de Máxima Seguridad – AMS- (Sala Cofre) para el equipamiento informático crítico en el Data Center del Gobierno de la Provincia de San Luis ubicado en la Ciudad de La Punta, de construcción modular constituida de paredes laterales, techo y estructura propia, que permita su ampliación.

El Ambiente de Máxima Seguridad (AMS) para el equipamiento informático crítico de la Autoridad Certificadora Provincial conforma un volumen de sellado hermético contra gases y vapores, aislamiento térmico, barrera de vapor contra la propagación de humedad y protección contra campos magnéticos.

El AMS genera un ambiente de un alto grado de protección contra siniestros, alta disponibilidad operacional, acceso restringido y controlado, así como un gerenciamiento preventivo de fallas ambientales.

CARACTERÍSTICAS DE LA SALA DEL AMS:

El objetivo de la Sala Cofre es el de proveer el mayor grado de protección posible para el nivel de operaciones críticas de la Autoridad Certificante provincial considerando las características particulares del lugar y edificio donde está emplazado. Y debe garantizar la protección contra el fuego, calor, magnetismo, humo, vapores, accesos indebidos, robo y vandalismo.

La Sala Cofre es un compartimiento ignífugo y hermético con características específicas para protección de equipamientos electrónicos, data centers, medios magnéticos, papeles y demás portadores de datos, con características de acuerdo a definición de NFPA, y

clasificado de acuerdo a UL-72 como Clase 125 – 2 horas. Esto quiere decir que un fuego externo de 1.000 °C durante 120 minutos no debe generar una temperatura interna mayor a 55 °C.

Es una solución estanca al agua exterior con resistencia al agua de extinción de incendio. Absolutamente estanco a los gases, humedad, penetración de polvo y/o agua presurizada mediante la implementación de una trampa de vapor.

Su puerta es a prueba de vandalismo, posee un sistema de puertas de acceso con cerramiento automático, un sistema de blindaje que permite el pasaje de cables y tuberías, y un sistema de sellado de juntas para proporcionar flexibilidad sin perder estanqueidad. Además posee características de construcción antisísmica Zona IV.

PUERTA DE ACCESO A LA SALA DEL AMS

El acceso se realiza a través de un sistema de puertas compuestas por capas de acero y aislantes. El cerramiento posee trabas automáticas y el accionamiento es electromecánico mediante la solución de control de accesos, pero totalmente libre para la salida (función antipánico que permita a las personas salir de la sala).

PISO TÉCNICO ELEVADO

Cuenta en su interior con piso elevado de acero relleno de concreto celular y revestimiento de laminado melamínico, que le dan mayor resistencia y tolera daños por uso pesado. Responde en sus características al Standard CISCA (Ceiling Interior & Construction Asociation) de EEUU, SPU Platform (Raised Access) Floors Performance Specification (UK).

Los paneles están totalmente recubiertos con un revestimiento superior de laminado plástico de alta resistencia al tránsito, antiestático y antideslizante.

ILUMINACIÓN DE LA SALA

La iluminación interna del AMS se brinda mediante paneles led con un nivel de iluminación con un valor aproximado de 500 lux. La que se complementa con una solución autónoma para iluminación de emergencia.

INSTALACIONES ELÉCTRICAS

El cableado eléctrico se distribuye mediante bandejas, y cuenta con un dimensionamiento acorde al requerimiento de potencia necesaria para el funcionamiento del equipamiento almacenado y protegido en la Sala Cofre.

SISTEMA AUTOMÁTICO DETECCIÓN Y SUPRESIÓN DE COMBUSTIÓN CON GAS FM 200.

El sistema está diseñado e instalado de acuerdo con las normas pertinentes de la NFPA, entre otras el estándar 2001.

El recinto del AMS está constituido por dos zonas de detección (ambiente y bajo piso), alarma y extinción automática basado en el agente extintor limpio FM-200/FE227. Dichas zonas están dotadas de detectores de humo convencionales, los cuales están dispuestos en zonificación cruzada, a fin de tener un mayor rango de detección de un incendio y evitando de esta manera, descargas innecesarias de agente extintor.

La solución posee distintos modos de operación automática. Como así también controles que permiten el bloqueo del proceso de conteo o temporización en curso para la propagación del gas.

Adicionalmente, el sistema cuenta con accionamiento manual, el cual provocará en forma inmediata y prioritaria la descarga de los depósitos de FM-200/FE227 en el

SISTEMA DE CLIMATIZACIÓN DE PRECISIÓN

Dados los estrictos requerimientos ambientales a mantener dentro de la sala cofre y debido a la alta criticidad del equipamiento contenido, se hace necesario contar con unidades de control ambiental de precisión para lograr su adecuada climatización. El control ambiental de precisión permite el estricto control de temperatura, humedad, distribución y pureza del aire las 24 horas del día, los 365 días del año. El mismo, está compuesto por módulos de alto desempeño y un elevado factor de sensibilidad al calor con redundancia 2N.

Esta solución cuenta con una unidad controladora que nos permite el monitoreo y gestión de alarmas antes las siguientes condiciones de sala: Temperatura, Humedad, alarmas audibles, ante distintas situaciones como pueden ser: Alta o baja temperatura, Alta o baja humedad, Falla de ventilador, Alta presión, Pérdida de energía, Problema de humidificador, entre otros.

SISTEMA CCTV

El Ambiente de Máxima Seguridad (AMS) cuenta con un Circuito Cerrado de Televisión o CCTV para el monitoreo y visualización del interior de la Sala Cofre. Mediante la instalación de un sistema de cámaras de seguridad se puede comprobar desde otra sala, y de manera remota, el funcionamiento y estado del AMS. Esta infraestructura nos permite que las imágenes captadas puedan ser supervisadas de forma remota por profesionales y el personal calificado del FDSL para detección de incidentes que afecten a la seguridad o al normal funcionamiento, como así también detectar cualquier anomalía, para evitar una intrusión indeseada.

Esta solución está disponible y grabando 24 horas al día, 365 días al año.

SOLUCIÓN MONITOREO

FDSL cuenta con una solución de monitorización especializada para entornos de TI de gran tamaño. Ofreciendo una visión centralizada orientada al servicio y permitiendo mapear procesos de negocio, consolidar paneles de varios servidores y supervisar el rendimiento y la disponibilidad de los acuerdos de nivel de servicio, entre otras funcionalidades. Esta herramienta nos ayuda a supervisar y analizar diferentes aspectos del sistema, como el consumo del ancho de banda o el estado de funcionamiento, y obtener datos de varios hosts como switches, routers, servidores y otros dispositivos y aplicaciones. Permitiendo que los administradores de red, por ejemplo, puedan estar al tanto del estado y el funcionamiento de los equipos y servicios que forman parte de la infraestructura, y recibir notificaciones cuando se produzcan anomalías o fallos en los mismos.

Con esta solución, también se permite monitorizar los recursos de hardware, como la carga del CPU, el espacio en disco, la memoria y el estado de los puertos. De esta forma, los administradores pueden optimizar el uso de los recursos y prevenir situaciones de sobrecarga o escasez. También dispone de una interfaz web adecuada para la resolución de problemas en tiempo real.

CONTROL DE ACCESO

El control de accesos se lleva a cabo mediante un sistema de última generación. Está compuesto por lectores de proximidad, lectores de tarjetas RFid, terminales autónomos de reconocimiento biométricos tanto facial como dactilar, controladora, sensores de puertas y cerraduras eléctricas y su correspondiente software de gestión el cual cuenta con las protecciones pertinentes para evitar el acceso indebido a personas no autorizadas. También cuenta con personal de seguridad calificado para el control de acceso inicial al ambiente de máxima seguridad.

ÁREAS ADMINISTRATIVAS SOPORTE DE LA INFRAESTRUCTURA DE FIRMA DIGITAL

Las áreas administrativas del Ambiente de Máxima Seguridad están definidas en base a los distintos niveles de acceso físico exigidos por la normativa provincial y nacional.

Se encuentran implementados siete niveles de acceso físico para el personal autorizado a ingresar y operar en el AMS. Con exigencias de autenticación y control crecientes a medida que se sube de nivel. Están supervisados por una combinación de personal de seguridad y cámaras de observación directa y grabación de eventos. Se define como:

Primer nivel: Desde el ingreso al edificio hasta la recepción del mismo en planta baja. En este nivel, se encuentra el Guardia de Seguridad, quien identifica y controla quién accede a los distintos sectores del edificio.

Segundo nivel: Este nivel está contiguo a la recepción. Nivel a partir del cual se encuentra el AMS. Su ingreso, está controlado por el Guardia de seguridad y solo se tiene acceso por cerradura con llave física convencional. La misma se encuentra en poder del personal operativo del AMS. El egreso de este nivel también debe ser documentado por el Guardia de Seguridad.

Tercer nivel: Control de acceso con huella dactilar que accede a la sala de operaciones. Los teléfonos celulares, así como otros equipos portátiles de comunicación, excepto aquellos exigidos para las operaciones de procesamiento de la Autoridad Certificante Provincial no son admitidos a partir de este nivel.

Cuarto nivel: El acceso está regulado por la combinación de lector biométrico de rostro y huellas digitales (pudiendo optar también por tarjeta de proximidad). A partir de este

nivel los ingresos deben de hacerse de manera dual por parte del personal autorizado a la operatoria del AMS.

Quinto nivel: Área donde se encuentra el equipamiento en AMS. El acceso está regulado por la combinación de lector biométrico de rostro y huellas digitales. Acá se encuentra el dispositivo criptográfico, los servidores del sistema de la Autoridad Certificante provincial y una caja fuerte compartimentada. El egreso de este nivel debe quedar registrado por sensor de salida.

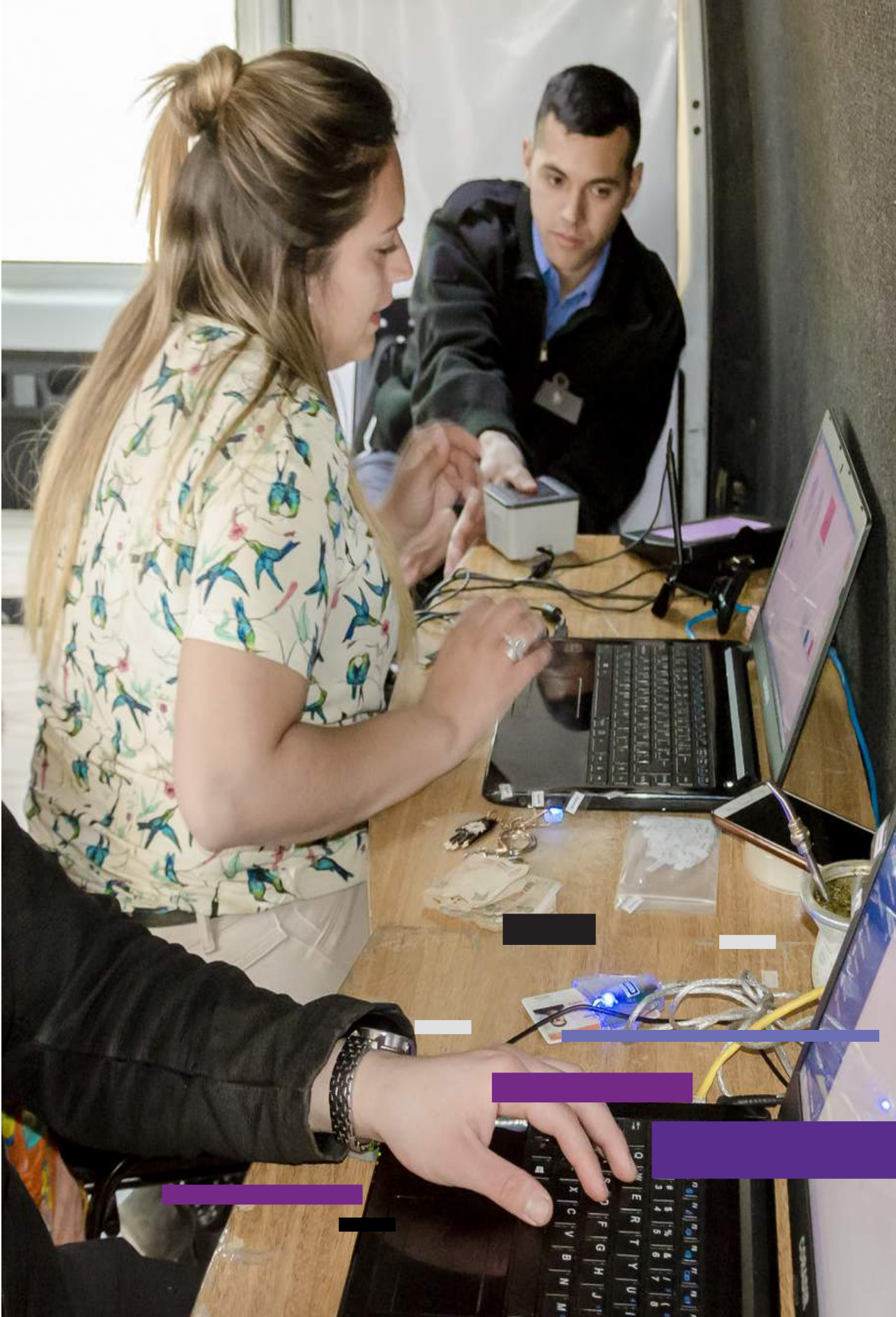
Sexto nivel: Caja Fuerte. Se requiere llave y combinación para su acceso/apertura.

Séptimo nivel: Compartimentos de la caja fuerte. Cada compartimento individual de la caja fuerte tiene su propia llave.

MIGRACIÓN Y ACTUALIZACIÓN DE TECNOLOGÍAS

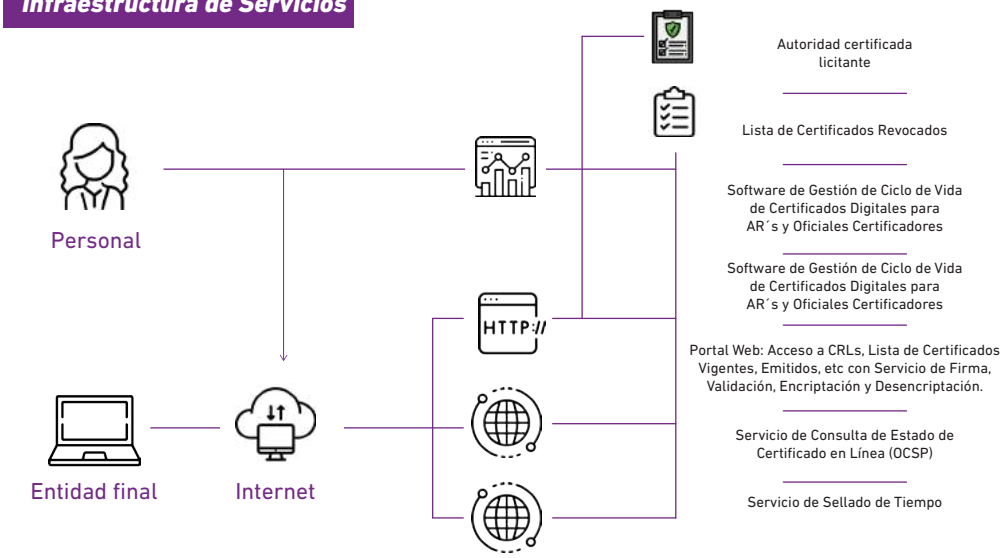
Con la experiencia adquirida durante los primeros 10 años de funcionamiento, FDSL planifica una actualización total de la infraestructura física y lógica realizando el llamado a la ***Licitación Pública N° 02/2018 "ADQUISICIÓN DEL DISEÑO E IMPLEMENTACIÓN DE UNA NUEVA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI) PARA LA PROVINCIA DE SAN LUIS, INCLUYENDO UN SOFTWARE DE ADMINISTRACIÓN DE LA INFRAESTRUCTURA DE CLAVE PÚBLICA Y LA ADQUISICIÓN DE HARDWARE PARA SU ARQUITECTURA, ADQUISICIÓN DE SOLUCIÓN DE BACKUP CON LIBRERÍA ROBÓTICA Y SOFTWARE"*** mediante la cual, se actualizó la totalidad de los componentes de redes, servidores y hardware criptográfico a la última tecnología y se reemplazó basándose en las buenas prácticas de seguridad el algoritmo SHA1 por SHA2 y el tamaño mínimo de claves de 1024 a 2048 bits (Precisamente SHA256 con RSA DE 2048 Bits).

De este modo se comenzaron a generar certificados digitales con claves de mayor tamaño lo que en la práctica trajo como consecuencia que los documentos así suscriptos sean más seguros y difíciles de adulterar. Dicha infraestructura se puso en funcionamiento en el año 2019.



La Autoridad de Certificación configurada y operacional permitirá a un sitio la emisión, el seguimiento, la administración, la revocación de certificados y emisión de CRL con mínima carga de administración y máxima seguridad.

Infraestructura de Servicios



Los servicios ofrecidos por el FDSL son:

- ***Servicio de OCSP (Protocolo de comprobación del estado de un certificado en línea).***

- ***Servicio de Sellado de Tiempo.***

- ***Servicio de portal web de la Autoridad Certificante Raíz Provincial.***

- ***Servicio de portal web de Autoridades Certificantes del Certificador Licenciado Provincial.***

- ***Software de la Autoridad de Registro (AARR) del Certificador Licenciante Provincial.***

Servicio OCSP (Protocolo en Línea del Estado de Certificado)

El "Protocolo en Línea del Estado de un Certificado" o "Online Certificate Status Protocol" es un servicio de verificación en línea del estado de los certificados. El OCSP es un método para determinar el estado de revocación de un certificado digital usando otros medios que no sean el uso de Listas de Revocación de Certificados (CRL). El resultado de una consulta a este servicio está firmado por el certificador que brinda el servicio.

El servidor OCSP se encuentra configurado en alta disponibilidad según RFC 6960.

Este servicio nos permite:

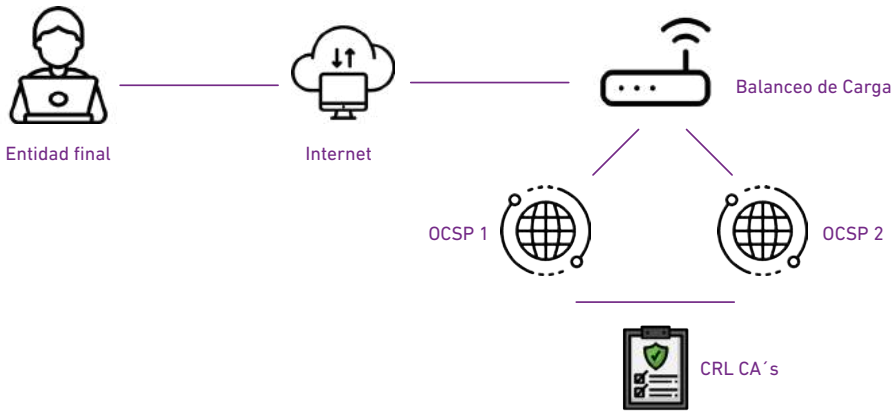
- ***Brindar información sobre el estado de certificados generados por una y/o todas las CA de la infraestructura.***

• Responder a peticiones de información sobre el estado de certificados digitales tanto a usuarios como a otros proveedores de servicios.

• Generar y custodiar las claves privadas utilizadas para firmar las respuestas, las que incluyen tanto la fecha como el estado del certificado.

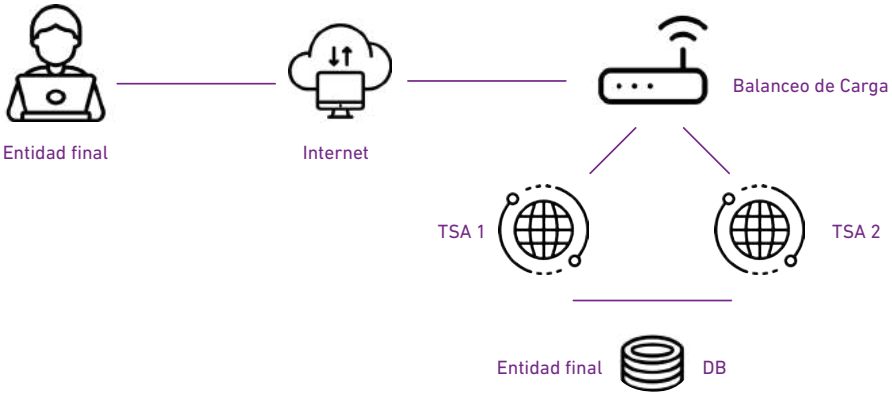
• Permitir el encaminamiento a un OCSP Responder externo.

• Operar en alta disponibilidad mediante mecanismo de balanceo de carga.



Servicio TSA (Sellado de Tiempo):

El sellado de tiempo o timestamping es un mecanismo en línea que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo. Este protocolo se describe en el RFC 3161 y está en el registro de estándares de Internet.
Una autoridad de sellado de tiempo actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora concreta.



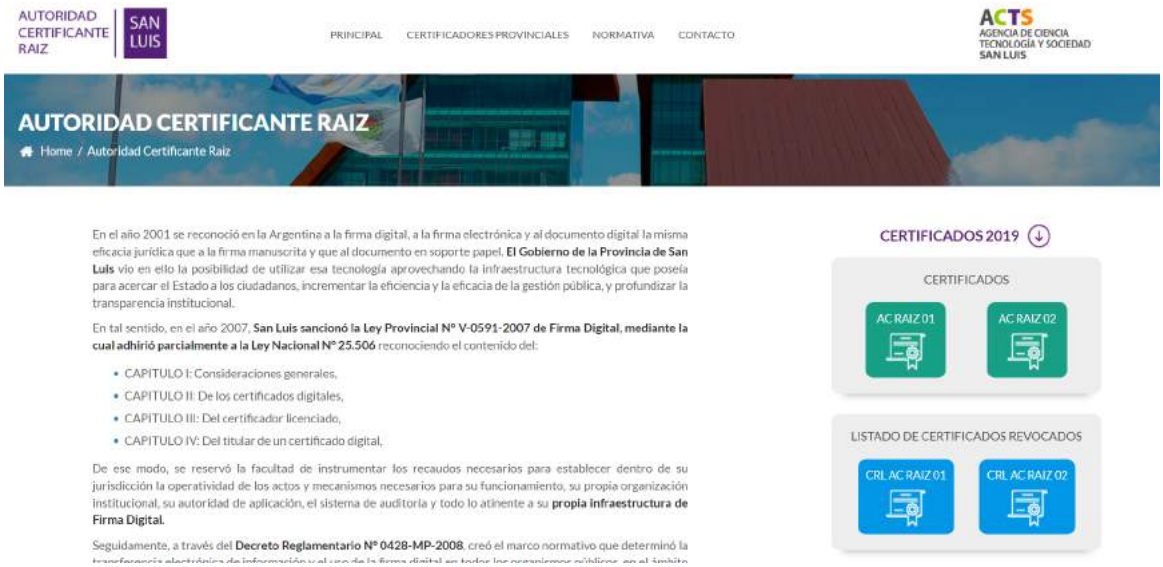
Servicio de portal web de la Autoridad Certificante Raíz

El portal web correspondiente a la Autoridad Certificante es compatible con todos los navegadores y opera en dispositivos móviles de manera responsiva según el tamaño de la pantalla.

Este sitio web se encuentra alojado en los servidores de Hosting del FDSL, desde donde publica la siguiente información:

- ***Lista de certificados revocados (CRL).***
- ***Lista de certificados vigentes.***
- ***Información y documentación relevante a cada política de certificación.***
- ***Información y documentación relevante a cada Certificador Licenciado Provincial y a sus políticas de certificación.***
- ***Información de la Autoridad Certificante Raíz y datos de contacto del Ente Licenciante Provincial.***

El portal del Ente Licenciante Provincial se encuentra disponible en el siguiente URL:
https://www.acraiz.sanluis.gov.ar/



Servicio de portal web de las Autoridades Certificantes Licenciadas Provinciales

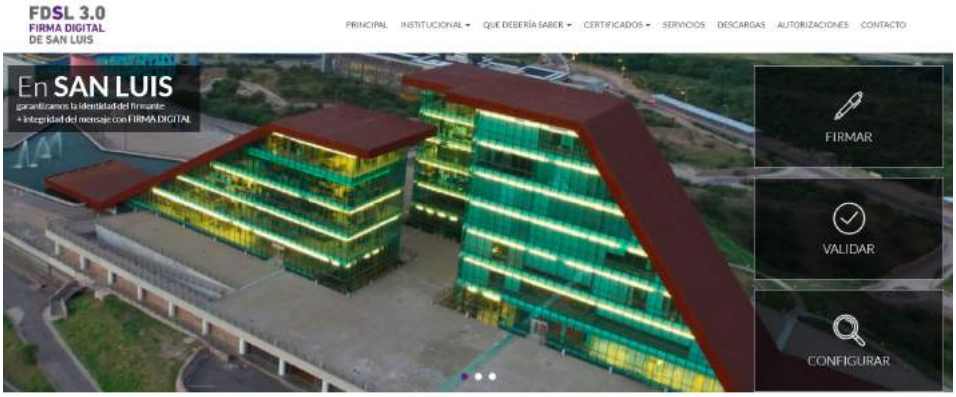
El portal web correspondiente a la Autoridad Certificante es compatible con todos los navegadores y opera en dispositivos móviles de manera responsiva según el tamaño de la pantalla.

Este sitio web se encuentra alojado en los servidores de Hosting del FDSL, desde donde publica la siguiente información:

- ***Lista de certificados revocados (CRL).***
- ***Lista de certificados vigentes.***
- ***Información y documentación relevante a cada política de certificación.***
- ***Información y documentación relevante a cada Certificador Licenciado Provincial y a sus políticas de certificación.***
- ***Información de la Autoridad Certificante Raíz y datos de***

contacto del Ente Licenciante Provincial.

El portal del Ente Licenciante Provincial se encuentra disponible en el siguiente URL:
https://www.acraiz.sanluis.gov.ar/



Software de la Autoridad de Registro (AARR) del Certificador Licenciado Provincial

El Instituto Firma Digital de San Luis ha implementado un software de Autoridad de Registro (AARR) robusto y eficiente para la gestión del ciclo de vida de los certificados digitales X.509 v3. Esta solución está diseñada sobre una plataforma completamente escalable, modular e integrable, que incluye un completo sistema de seguridad diseñado según las normativas de la provincia de San Luis.

Dichas recomendaciones afectan a los requisitos de seguridad y operación de los Sistemas Confiables de Gestión de Certificados Digitales y Firma Electrónica.
La solución es del tipo sistema de expedientes, esto nos permite representar todos y cada uno de los procesos involucrados, en actuaciones de un expediente electrónico con firma digital. Generándose un expediente electrónico

por cada solicitud de Certificado Digital. Dicha solución nos permite gestionar un gran volumen de datos de forma segura, fiable y eficiente.

A través de esta solución también podemos realizar la administración de la PKI permitiéndonos, por ejemplo:

• Emitir, rechazar y revocar certificados de clave pública, según el estándar X.509v3. Publicar las correspondientes Listas de Certificados Revocados (CRL).

• Gestionar un módulo de administración general de sistema.

• Gestionar las altas, bajas y modificaciones de Usuario, organismos, dependencias, autoridades de registro, entre otros.

• Gestionar un módulo de Auditorías relacionado a calidad ISO 9001.

• Revisar los registros de auditoría en busca de incidentes de seguridad.

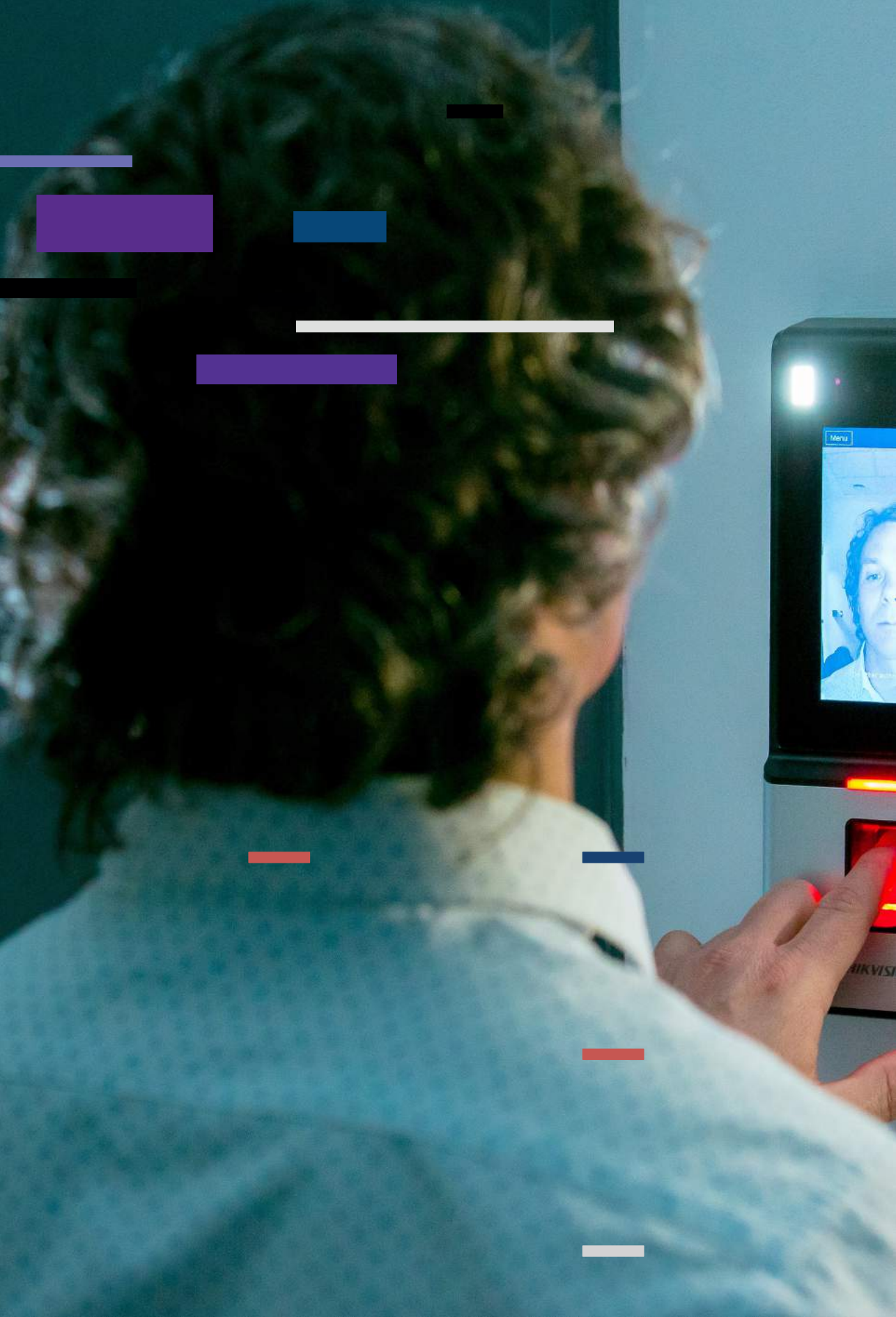
• Gestionar un módulo de reportes y estadísticas.

• Garantizar el acceso seguro al mismo, mediante el uso de dispositivos criptográficos como medios de acceso.

• Tener más de 200 Oficiales de registros conectados recurrentemente.

• Integrarse al sistema de Cédula de Identidad Provincial Electrónica (CIPE) de la provincia de San Luis permitiendo el uso de web services existentes.

CIPE 4.0
CÉDULA DE IDENTIDAD
ELECTRÓNICA
hp


Menu

7

SEGURIDAD Y REDUNDANCIA DE LA INFRAESTRUCTURA DE FIRMA DIGITAL

CIPE 4

SEGURIDAD Y REDUNDANCIA DE LA INFRAESTRUCTURA DE FIRMA DIGITAL

El Instituto Firma Digital de San Luis ha implementado una infraestructura robusta compuesta por tres plataformas distintas: Producción, Testing/Capacitación y Contingencia.
La plataforma de Testing/Capacitación es el primer escenario donde se despliegan las soluciones a implementar. Esta plataforma, que replica fielmente las características de la solución productiva, permite evaluar nuevas funcionalidades sin interferir con el funcionamiento de la plataforma productiva. Cuando se identifica un nuevo requerimiento, éste se documenta, analiza y clasifica. Los requerimientos considerados necesarios se ponderan y cotizan para su aprobación e incorporación.
Una vez desarrolladas, las nuevas funcionalidades se despliegan en la plataforma de Testing para su validación. Tras confirmar su correcto funcionamiento, se ponen a disposición de los interesados para su capacitación. Posteriormente, tras la aprobación, se despliegan en la plataforma de Producción.
Esta plataforma también es utilizada a fin de capacitar a los Oficiales de Registro, responsables de operar en cada una de las más de 80 Autoridades de Registro que FDSL posee constituídas.
En la plataforma de Producción, las nuevas funcionalidades pasan a ser de uso cotidiano. Aquí es donde se pueden detectar o generar nuevas necesidades, lo que permite gestionar un sistema de mejora continua.
Finalmente, la plataforma de Contingencia actúa como un respaldo en caso de cualquier eventualidad que pueda afectar a las otras dos plataformas.
Cada despliegue en cada plataforma se documenta en un registro versionado, asegurando así un seguimiento detallado de todas las actualizaciones y cambios realizados.

Los módulos criptográficos son componentes vitales en la seguridad informática, facilitando operaciones criptográficas como el cifrado y descifrado de información, generación y verificación de firmas digitales, y creación de claves criptográficas. Estos pueden ser hardware o software, y su objetivo es garantizar la confidencialidad e integridad de los datos.

Es crucial que los módulos criptográficos cumplan con estándares de seguridad establecidos, como el FIPS 140-2. Este estándar garantiza la confidencialidad, integridad y disponibilidad de la información protegida mediante criptografía. Define cuatro niveles de seguridad que se aplican según el tipo y sensibilidad de los datos manejados, así como el entorno y las amenazas a las que se enfrentan.

Los dispositivos criptográficos son herramientas esenciales para garantizar la seguridad informática. Entre los más comunes se encuentran los Hardware Security Modules (HSM), tarjetas inteligentes y tokens USB. Los HSM ofrecen un nivel extra de seguridad al realizar operaciones criptográficas delicadas. Las tarjetas inteligentes y tokens USB son portátiles y se utilizan en aplicaciones como autenticación de usuarios y firma digital.

HID

En SAN LUIS
FIRMAR
VALIDAR
CONFIGURAR
929722 Certificados emitidos
Personas Humanas
Personas Vinculadas
Agentes del Estado

INFRAESTRUCTURA NETWORKING

La infraestructura de red del FDSL es bastante robusta y está diseñada para ofrecer alta disponibilidad y rendimiento.

La red está basada en una arquitectura mallada, lo que significa que todos los nodos están interconectados. Esto proporciona redundancia, ya que, si una conexión falla, los datos pueden ser reenrutados a través de las múltiples conexiones restantes. Esto es crucial para mantener la alta disponibilidad.

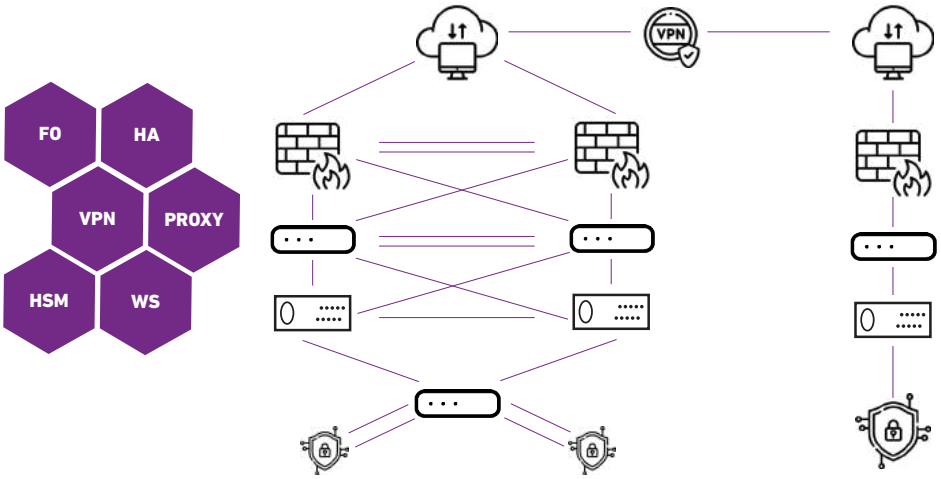
Los firewalls actúan como la primera línea de defensa contra las amenazas de seguridad. Estos dispositivos de seguridad, de alto rendimiento, inspeccionan el tráfico entrante y saliente y aplican las políticas de seguridad necesarias.

Éstos se complementan con switches que gestionan el tráfico de la red interna. La red utiliza conexiones de fibra óptica y Gigabit Ethernet para garantizar velocidades de transmisión de datos rápidas y confiables. La fibra óptica es especialmente útil para conexiones a larga distancia, mientras que el Gigabit Ethernet proporciona una conectividad sólida para distancias más cortas.

Los servidores son la columna vertebral de esta infraestructura. Ofrecen un alto rendimiento y son conocidos por su eficiencia energética y su capacidad para manejar cargas de trabajo intensivas.

Finalmente, los HSM se utilizan para proteger las claves y realizar operaciones criptográficas. Éstos dispositivos son esenciales para mantener la integridad y la seguridad de los datos.

En resumen, esta infraestructura de red combina hardware de alta calidad con una arquitectura bien pensada para proporcionar un servicio de red altamente disponible, rápido y seguro.



La red está basada en una arquitectura virtualizada, justamente con más de cien servidores virtualizados. Estos servidores alojan máquinas virtuales que ejecutan diversos sistemas operativos, incluyendo Microsoft Windows Server y Linux Ubuntu.

Entre los componentes de esta infraestructura se encuentran las autoridades certificadoras, que emiten y gestionan los certificados digitales utilizados para la autenticación y el cifrado. Los servidores proxy se utilizan para intermediar las comunicaciones entre los clientes y los servidores, mejorando la seguridad y el rendimiento.
Los servidores DNS se encargan de la resolución de nombres de dominio, mientras que los servidores NTP proporcionan una sincronización precisa del tiempo. Los servidores web alojan las aplicaciones y sitios web accesibles a través de la red.

Los balanceadores de carga distribuyen el tráfico de la red entre varios servidores para optimizar el rendimiento y la disponibilidad. Los sistemas publicadores se encargan de publicar contenido en la web.

Finalmente, las bases de datos SQL almacenan y gestionan

los datos utilizados por las aplicaciones y servicios de la red.

Solución de backup y Restauración

Esta solución de red también incluye un plan de respaldo exhaustivo. Los respaldos se realizan con una frecuencia variada para garantizar que los datos estén protegidos en todo momento: diariamente, semanalmente, mensualmente, trimestralmente, semestralmente y anualmente.

Además de los respaldos digitales, también se realizan respaldos a cinta utilizando una librería robótica. Estos respaldos a cinta proporcionan una capa adicional de seguridad y son especialmente útiles para la recuperación de desastres.

Los respaldos se almacenan en diferentes lugares siguiendo la lógica de 3-2-1-0:

- ***3 copias de datos diferentes: Esto asegura que siempre haya múltiples copias de los datos en caso de que una copia falle o se corrompa.***
- ***2 medios diferentes: Los datos se almacenan tanto en medios digitales como en cinta para proteger contra diferentes tipos de fallos.***
- ***1 copia remota y 1 copia offline: Una copia de los datos se almacena fuera del sitio para proteger contra desastres locales. Además, una copia se mantiene offline para proteger contra amenazas como el ransomware.***
- ***3 lugares distintos: Esto proporciona redundancia geográfica y protege contra desastres que podrían afectar a una sola ubicación.***
- ***0% errores: Todos los respaldos son verificados para asegurar que pueden ser recuperados sin errores.***

En resumen, esta solución de respaldo proporciona una protección completa y robusta para los datos en esta infraestructura de red. Con múltiples capas de redundancia y protección contra una variedad de amenazas, pudiendo estar seguro de que los datos están seguros.

Después de realizar los respaldos, se llevan a cabo pruebas de restauración tanto del almacenamiento como de las cintas. Estas pruebas son esenciales para verificar que los respaldos se han realizado correctamente y que los datos pueden ser recuperados en caso de necesidad.
Durante la prueba de restauración del almacenamiento, se intenta recuperar los datos del almacenamiento digital. Esto verifica que los datos no se hayan corrompido durante el proceso de respaldo y que el hardware de almacenamiento esté funcionando correctamente.

La prueba de restauración de cintas implica intentar recuperar los datos de las cintas de respaldo. Dado que las cintas son un medio más antiguo y físico, estas pruebas son especialmente importantes para asegurar que las cintas no se hayan dañado y que los datos puedan ser recuperados.

Estas pruebas de restauración son una parte crucial del plan de respaldo. No sólo verifican que los respaldos se estén realizando correctamente, sino que también aseguran que los datos puedan ser recuperados en caso de una emergencia. Estas pruebas proporcionan una capa adicional de seguridad y tranquilidad.

Solución de contingencia

La infraestructura de red descrita anteriormente cuenta con un plan de contingencia integral diseñado para garantizar la continuidad del servicio en caso de cualquier eventualidad. Este plan de contingencia es seguro, fiable y robusto, proporcionando una capa adicional de protección para los datos y servicios críticos.

El plan de contingencia mantiene en existencia capacidades externas de procesamiento fuera del lugar donde reside el Sistema Informático productivo de las Autoridades Certificantes de la infraestructura puntana e incluye un ambiente de máxima seguridad idéntico a la infraestructura principal. Este ambiente está siempre listo para asumir el control en caso de una falla en la infraestructura principal. Al ser una réplica exacta, puede manejar las mismas cargas de trabajo y ofrecer el mismo nivel de rendimiento y seguridad.

En caso de una falla o un problema en la infraestructura principal, el tráfico de la red puede ser redirigido rápidamente a este ambiente de contingencia. Esto asegura que los servicios de red permanezcan disponibles incluso durante los eventos de interrupción.

Este ambiente de contingencia también es útil para realizar pruebas y actualizaciones sin afectar la infraestructura principal. Por ejemplo, antes de implementar una actualización en la infraestructura principal, se puede probar primero en el ambiente de contingencia.

En resumen, este plan de contingencia proporciona una protección completa y robusta para la infraestructura de red. Con múltiples capas de redundancia y protección contra una variedad de amenazas, proporcionando una solución robusta para cualquier eventualidad y garantizando que los datos están seguros y tus servicios disponibles.

CIPE 4.0

CÉDULA DE IDENTIDAD PROVINCIAL ELECTRÓNICA (CIPE)

CÉDULA DE IDENTIDAD PROVINCIAL ELECTRÓNICA (CIPE)

Es la cédula de identidad de los habitantes de la Provincia de San Luis.

Además de la identificación física, permite la identificación digital de su titular y la firma digital.

Su apariencia es similar a la de una tarjeta de crédito, e incorpora un chip criptográfico que contiene la información básica para acreditar electrónicamente la identidad de su titular y la firma de documentos electrónicos con plena validez legal.

Para las personas que así lo soliciten, la CIPE incluirá en el mismo soporte (tarjeta inteligente) la licencia de conducir (CIPE-LC).

En en 2009, a través de la Ley Provincial Nº V-0698-2009 - LEY DE CÉDULA DE IDENTIDAD PROVINCIAL ELECTRÓNICA - se crea la Cédula de Identidad Provincial Electrónica (CIPE) con la finalidad de contener en una misma cédula todos los datos necesarios para la identificación de la persona, tanto física como digitalmente.

Garantizando la protección de los datos personales de su titular. Asimismo se prevé la posibilidad de firmar digitalmente documentos públicos y privados.

La infraestructura de red descrita anteriormente cuenta con un plan de contingencia integral diseñado para garantizar la continuidad del servicio en caso de cualquier eventualidad. Este plan de contingencia es seguro, fiable y robusto, proporcionando una capa adicional de protección para los datos y servicios críticos.

El plan de contingencia mantiene en existencia capacidades externas de procesamiento fuera del lugar donde reside el Sistema Informático productivo de las Autoridades Certificantes de la infraestructura puntana e incluye un ambiente de máxima seguridad idéntico a la infraestructura principal. Este ambiente está siempre listo para asumir el control en caso de una falla en la infraestructura principal. Al ser una réplica exacta, puede manejar las mismas cargas de trabajo y ofrecer el mismo nivel de rendimiento y seguridad.

En caso de una falla o un problema en la infraestructura principal, el tráfico de la red puede ser redirigido rápidamente a este ambiente de contingencia. Esto asegura que los servicios de red permanezcan disponibles incluso durante los eventos de interrupción.

Este ambiente de contingencia también es útil para realizar pruebas y actualizaciones sin afectar la infraestructura principal. Por ejemplo, antes de implementar una actualización en la infraestructura principal, se puede probar primero en el ambiente de contingencia.

En resumen, este plan de contingencia proporciona una protección completa y robusta para la infraestructura de red. Con múltiples capas de redundancia y protección contra una variedad de amenazas, proporcionando una solución robusta para cualquier eventualidad y garantizando que los datos están seguros y tus servicios disponibles.

MINISTERIO
DE CIENCIA
Y TECNOLOGÍA
CIPE 4.0
CÉDULA DE IDENTIDAD
PROVINCIAL ELECTRÓNICA
SAN LUIS

CIPE
4.0

9

INFRAESTRUCTURA Y CENTROS DE EMISIÓN. CANTIDAD Y DISTRIBUCIÓN

INFRAESTRUCTURA Y CENTROS DE EMISIÓN. CANTIDAD Y DISTRIBUCIÓN

En el año 2010, el proyecto de la Cédula de Identidad Provincial Electrónica (CIPE) dio inicio con la apertura de 3 Centros de Emisión, siendo el primero de ellos ubicado en la Unidad Regional III de Concarán.

En diciembre de 2015, al inicio del mandato del Gobernador Alberto Rodríguez Saá, la CIPE contaba con 22 Centros de Emisión en funcionamiento. En este periodo, la administración de la CIPE fue transferida al Ministerio de Ciencia y Tecnología. A lo largo de los siguientes 8 años de gestión, el Programa CIPE/Licencia de Conducir experimentó un crecimiento significativo, alcanzando la notable cifra de 51 Centros de Emisión.

Este incremento se llevó a cabo bajo constantes evaluaciones de ubicaciones estratégicas, asegurando una distribución equitativa para llegar a toda la población provincial. Todo esto, con el objetivo de optimizar la accesibilidad de los ciudadanos a los servicios de emisión de CIPE.

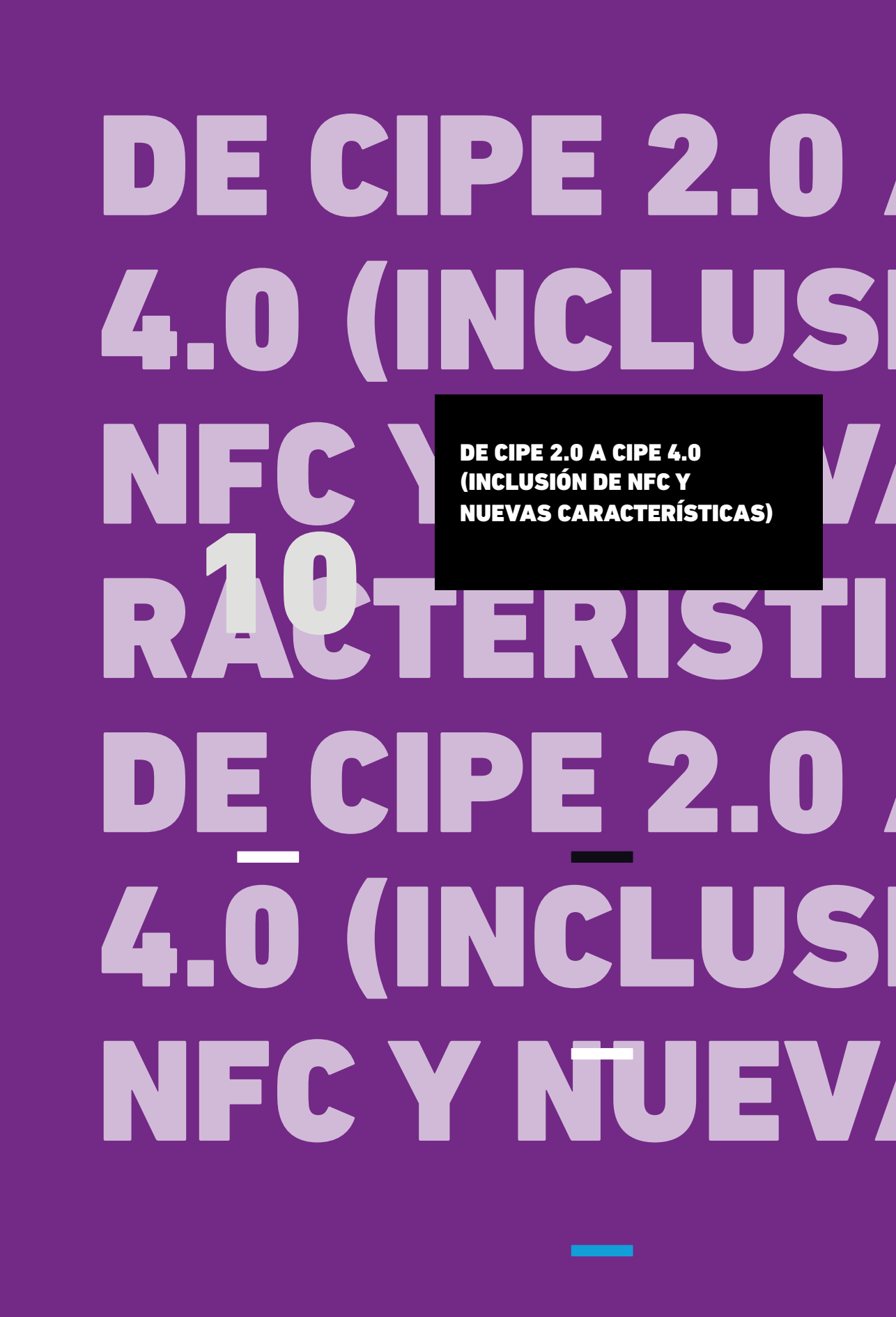
Es importante destacar que, junto con la expansión en el número de centros, se llevó a cabo una mejora sustancial en la capacidad de atención de cada uno de ellos, contribuyendo así a una mayor eficiencia y accesibilidad para los ciudadanos que buscan obtener su CIPE. Este avance no solo implica un incremento cuantitativo, sino también una optimización cualitativa en la prestación de servicios relacionados con la identificación y documentación provincial.

EDIFICIO ADMINISTRATIVO (EX CASA DE GOBIERNO)	ANCHORENA
EDIRO (TERMINAL DE ÓMNIBUS)	PASO GRANDE
JEFATURA CENTRAL DE POLICÍA (SAN LUIS)	SAN GERÓNIMO
CENTRO CÍVICO (VILLA MERCEDES)	TILISARAO
JEFATURA DE POLICÍA UR II (VILLA MERCEDES)	LA CALERA
VILLA DE MERLO	UNIÓN
JUANA KOSLAY	BEAZLEY
LA PUNTA	BALDE
QUINES	ZANJITAS
SAN FRANCISCO DEL MONTE DE ORO	NASCHEL
LA TOMA	LA PUNILLA
CONCARÁN	ARIZONA
LOS MOLLES (JUNIN)	NOGOLI
EL VOLCÁN	LOS MANANTIALES
EL TRAPICHE	PAPAGAYOS
VILLA LARCA	CARPINTERIA
NUEVA GALIA	FORTUNA
SAN MARTÍN	VILLA DEL CARMEN
CANDELARIA	TERRAZAS DEL PORTEZUELO
POTRERO DE LOS FUNES	LAS VERTIENTES
LAFINUR	FORTÍN EL PATRIA
RENCA	LUJÁN
CORTADERAS	NAVE CULTURAL (EX SCAC)
SAN PABLO	

Además se realizaron visitas de CIPE Móvil (vehículo adaptado para realizar emisiones in situ) y operativos de emisión en encuentros, organismos, localidades y barrios.

LUIS
PRADA

CPE 3.0


DE CIPE 2.0 A
4.0 (INCLUSI
NFC Y NUEVA
RACTERISTI
10
DE CIPE 2.0 A
4.0 (INCLUSI
NFC Y NUEVA
DE CIPE 2.0 A CIPE 4.0
(INCLUSIÓN DE NFC Y
NUEVAS CARACTERÍSTICAS)

CORADIR

DE CIPE 2.0 A CIPE 4.0 (INCLUSIÓN DE NFC Y NUEVAS CARACTERÍSTICAS)

La Cédula de Identidad Provincial Electrónica (CIPE) tiene como finalidad contener en una misma cédula todos los datos necesarios para la identificación de la persona, tanto física como digitalmente. La CIPE comienza su emisión en el 2010, posibilitando la identificación en línea y la Firma Digital a través del chip criptográfico incluido.

LAS PRIMERAS CÉDULAS FUERON EMITIDAS EN NOVIEMBRE DEL 2010 EN CONCARÁN. EN ESE AÑO SE EMITIERON UN TOTAL DE 972 CÉDULAS.

DESDE SU COMIENZO (NOVIEMBRE 2010) HASTA LA IMPLEMENTACIÓN DE LA CIPE 3.0 (17 DE MARZO DEL 2017) SE EMITIERON UN TOTAL DE 151.412 CÉDULAS.

En marzo de 2017 se actualizó la CIPE a la nueva CIPE 3.0 con tecnología NFC (Near Field Communication) que permite a los habitantes de San Luis firmar digitalmente desde dispositivos móviles que posean la misma tecnología, posibilitando la interacción entre personas, empresas y gobierno.

CÉDULAS EMITIDAS EN TOTAL DESDE EL 17/03/2017: 366387

SOLO LICENCIAS DE CONDUCIR (CLC) DESDE 17/03/2017: 60823

SOLO CIPE DESDE EL 17/03/2017: 31259

CIPE CON PASE LIBRE: 8666

HISTORIA

AÑO	CIPEs EMITIDAS
2010	972
2011	34652
2012	25061
2013	27529
2014	18269
2015	23017
2016	18063
2017	87809
2018	101834
2019	86954
2020	23774
2021	35697
2022	38213
2023	27326

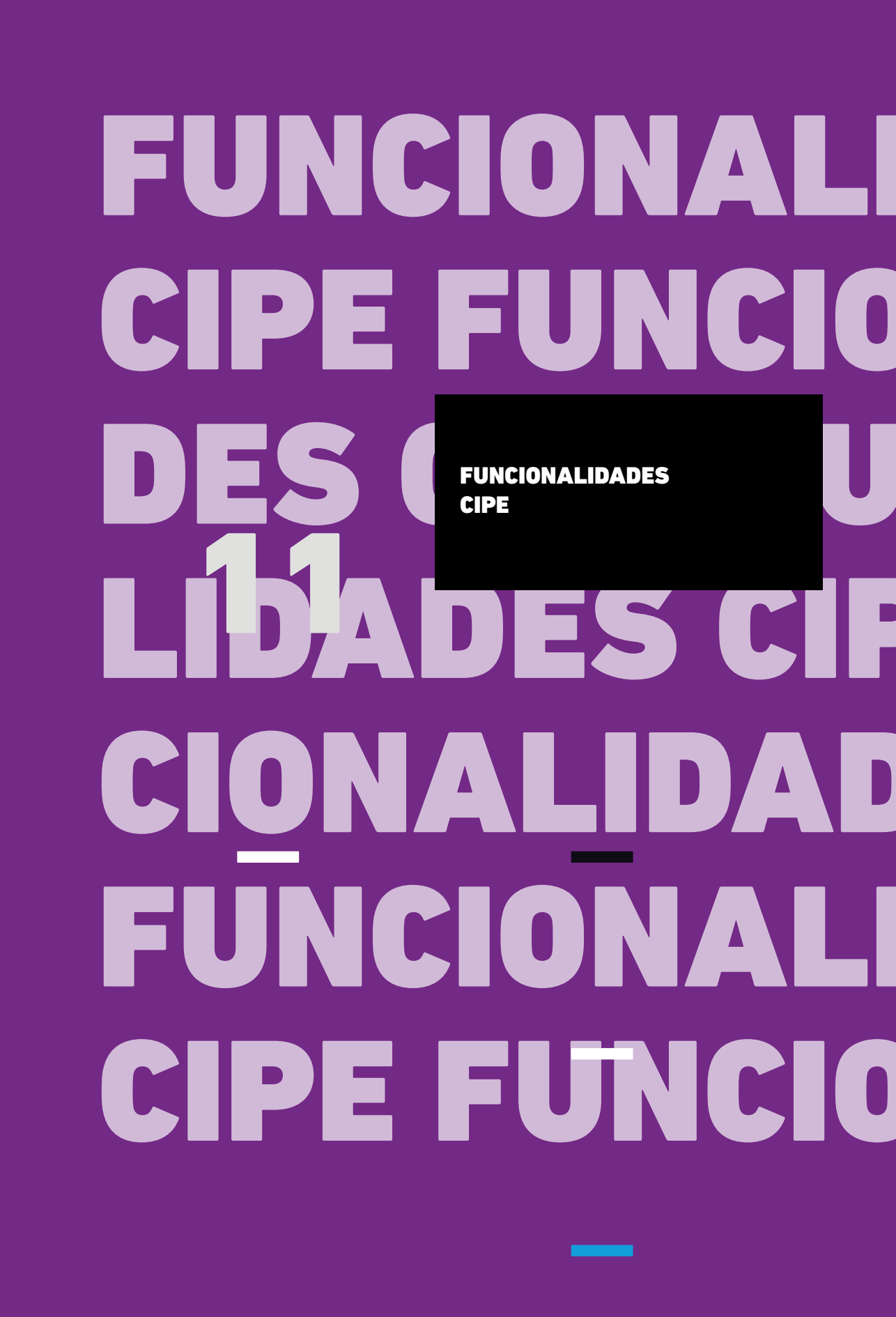
CIPE 4.0 LC Nación

En mayo de 2023 se emitió la primera CIPE 4.0 integrada a los estándares del Sistema Nacional de Licencias de Conducir. El Gobierno provincial firmó un Convenio con la Agencia Nacional de Seguridad Vial (ANSV) sumando CIPE/Licencia de Conducir al Sistema de Licencia Nacional respetando el sistema y formato con el que actualmente cuenta San Luis.

El convenio implicó los mismos requisitos y categorías que Nación. La implementación del Certificado Nacional de Antecedentes de Tránsito (CeNAT). De esta manera, previo a la emisión de una licencia de conducir se consulta la información existente en los Registros Nacionales de Antecedentes.

Las políticas implementadas en materia de Seguridad Vial apuntan a la coordinación y armonización entre todas las jurisdicciones, con el objetivo final de disminuir los índices de siniestralidad vial.

PERSONAS CON CIPE, CIPELC O CIPELN: 325436


FUNCIONALI
CIPE FUNCIO
DES C U
LIDADES CIP
CIONALIDAD
FUNCIONALI
CIPE FUNCIO
11
FUNCIONALIDADES
CIPE

CIPE 4.0
SAN LUIS
CIPE 4.0
CÉDULA DE IDENT
PROVINCIAL ELECT
CIPE 4.0

FUNCIONALIDADES CIPE

A través del portal de trámites www.puntano.gob.ar los habitantes de San Luis pueden realizar trámites de forma remota con firma digital.

Aplicaciones como Comisaría Virtual, Portal Puntano, Alarma Puntana y Registros Médicos. Son específicas para médicos, policías y docentes que se valen de la para confirmar la identidad de los usuarios y firmar digitalmente.

Comisaría Virtual, trámites que se pueden realizar: Certificado de domicilio, Certificado de estadía, Certificado de supervivencia, Constancia por extravío, Certificado de antecedentes, Exposición Ciudadana, Denuncia Ciudadana.

Portal Puntano, Portal Puntano es el portal de trámites Online de la Provincia de San Luis. Se puede realizar diversas gestiones tales como: acceder a partida de nacimiento, registros médicos, mapa deportivo, Sistema de Gestión de Educación, Expedientes Judiciales, los empleados estatales pueden acceder a su recibo de sueldo; así como también se puede realizar solicitud de turnos de organismos del estado.

Alarma Puntana, es una aplicación para teléfono móvil con la cual podrás dar aviso a la policía, pedir una ambulancia, informar un incendio, violencia o cuestiones ambientales. Para poder utilizarla se obtiene una clave en cualquier centro de emisión de CIPE de la Provincia de San Luis.

La Obra Social Estatal (DOSEP), estableció que CIPE es el carnet para realizar los trámites que en este organismo se realizan.

El Ente Control de Rutas, estableció que con CIPE los residentes de San Luis obtienen descuentos en los peajes provinciales.

CUD (Certificado Único de Discapacidad)

Las personas que cuenten con el Certificado lo pueden incluir en CIPE. Con la leyenda "Carnet CUD" seguida por el número del certificado único de discapacidad. Ese carnet tendrá el mismo plazo de vigencia que el CUD. Es decir, si a una persona que padece una discapacidad le fue expedido un CUD con fecha de vencimiento el 01/01/2020, el Carnet CUD tendrá validez hasta el 01/01/20, sin necesidad que la persona se presente a renovarlo periódicamente.
Además, las personas que cuenten con pase libre por salud para poder usar el transporte público de pasajeros lo pueden incorporar en su cédula.

Credenciales Policiales

El Instituto de Firma Digital y la Policía de la Provincia firmaron un convenio de colaboración, por el cual la Policía se constituye como Autoridad de Registro de Firma Digital. Los certificados de firma se cargarán en las nuevas credenciales con las que contará la Policía, basadas en la misma tecnología que la CIPE 3.0.

La nueva credencial policial será necesaria para utilizar las tabletas con NFC que entregará el Gobierno de la Provincia. Desde el Ministerio de Ciencia y Tecnología indicaron que para acceder al plan de entrega de tabletas, los policías tienen como requisito contar con la nueva credencial policial 3.0.

Credenciales Penitenciarios

Además de servir como método de identificación personal, en la documentación de formato vertical figura la portación de sus armas reglamentarias.

Tiene características de seguridad que la hacen inviolable y la información del personal se centraliza en el Data Center de la Provincia.

Credenciales Veteranos

Hemos realizado una mejora en el diseño de la CIPE 4.0 destinada a los Héroes de Malvinas y viudas, que consiste en la inclusión de una representación gráfica de las Islas Malvinas junto con una leyenda que les rinde tributo. Deseamos facilitar cualquier trámite que deban realizar, simplificándolo en un único documento. Por ejemplo, esto incluye el acceso al transporte público de pasajeros, brindándoles la comodidad que se merecen.

Tipos de credenciales:

• Credenciales para Ex Combatientes, Héroes de la Guerra, de Islas Malvinas e Islas del Atlántico Sur, según Ley N° I-0859-2013 y viudas.
• Credenciales para Ex Combatientes, Héroes de la Guerra, de Islas Malvinas e Islas del Atlántico Sur, según Ley N° 23.848-1990.
• Credenciales para Soldados de la Brigada Heroica en el marco del Derecho de Inclusión Social, según Ley N° I-0984-2017 y viudas.
• Credenciales para Soldados Continentales Del Atlántico Sur.

12

CERTIFICACIONES INTERNACIONALES

San Luis Argentina

CERTIFICACIONES INTERNACIONALES

El Instituto de Firma Digital de San Luis ha logrado un hito significativo en su compromiso con la calidad y la seguridad de la información. Recientemente, el instituto ha obtenido las certificaciones ISO 9001:2018 e ISO 20000-1:2011. La certificación ISO 9001:2018 es un estándar internacional que demuestra la capacidad de una organización para proporcionar productos y servicios que cumplen con los requisitos del cliente y los reglamentos aplicables. Por otro lado, la certificación ISO 20000-1:2011 es un estándar de servicio específico que demuestra la excelencia y demuestra las mejores prácticas en la gestión de servicios de TI. Estas certificaciones son un testimonio del compromiso del instituto con la mejora continua, la satisfacción del cliente y la entrega de servicios de TI de alta calidad.

Además, el Instituto está actualmente en camino a obtener la certificación ISO 27001. Esta es una norma internacional que se centra en la seguridad de la información, proporcionando requisitos para un sistema de gestión de seguridad de la información (SGSI). Al obtener esta certificación, el instituto demostrará su compromiso con la protección de la información y los datos, reforzando aún más su reputación como líder en el campo.

En cuanto a CIPE, obtuvo su primera certificación bajo normas internacionales de estandarización durante el año 2018. El sistema de Gestión de la Calidad cumple con los requisitos de la norma IRAM - ISO 9001:2015 y alcanza los procesos de "Emisión, renovación, duplicado o actualización de CIPE (Cédula de Identidad Provincial Electrónica de Identificación Física y Digital, Firma Digital y acceso virtual a la plataforma de servicios del Gobierno de San Luis), CIPE/CUD (Discapacidad), CIPE/SALUD, CIPE/CUCAI (Ablación e Implantes) y CIPE/LC (Licencia de Conducir), en la provincia de San Luis a través de la Red de Centros de Emisión CIPE". Certificado que mantiene hasta la actualidad.

ASOCIACION VETERANOS DE GU
MALVINAS ARGENTINAS

CRÉDITOS

13

CRÉDITOS

ISNB 978-987-1760-83-1

Directora
Luciana Rosario Vera

Gerente de Infraestructura Tecnológica
Marcos Esteban Hauria Hehn

Responsable de Normativa Jurídica
María Jesús Bálzola Etcheverry

Coordinadora de Auditorías
Veronica María Luz Morales Jofre

Vinculador
César Gastón Marilungo

Responsable Auditor CIPE-LC
Dania Ingrid Flores Flandez

Oficial de Registro Central
Jose federico Orozco

Responsable de Sistemas AARR
Luis Ramiro Alaniz

Responsable Auditor FDSL
Emanuel Cano

Oficial Mesa de Ayuda AR Central
Cristian Emilio Tissera Cerutti

Responsable de Operación Técnica
Pedro Roberto Presilla Salazar

Responsable de Operación Técnica
Jonathan Molina

Responsable de Sistemas
Rodrigo Dominguez

Responsable de Sistemas
Abel Zeballo

Responsable de Sistemas
Mariano Alberto Giannini

Responsable de Sistemas
Fernando Roucco

Responsable de Telecomunicaciones
Ariel Alejandro Giménez

Responsable de Telecomunicaciones
Franco Videla

Responsable de Seguridad Informática
Diego Agüero

Responsable de Infraestructura Edilicia
Enrique Quiroga

Responsable de Infraestructura Edilicia
Jesús Bertín

Gerente CIPE Licencia de Conducir
Nicolás Rodríguez Iannello

Vinculación con la Sociedad:
Gisela Parcio

Recursos Humanos
Romina Arancibia Rodriguez

Soporte Técnico y Logística
Fabián Sindoni

Equipo Técnico
Lucas Santiago Antunez
Florencia Guerrier
Kevin Diaz
Graciela López
Claudia Perez
Franco Orlando
Renzo Funes
Karim Dip
Santiago Diaz
Felipe González Gola
Virginia Gatica
Ailen Gimenez
Daniela Morales
Dania Flores

Mención especial
a todas las operadoras y operadores de CIPE que hacen posible este proyecto.

Coordinación General
Emanuel Lorenzoni

Edición y corrección
Pedro Bazán

Diseño
Tania Gialluca

Fotografía
Axel E. Seleme
Nicolás Varvara
Cristina Fernandez

Universidad de La Punta
ULP Virtual / 1a ed. - La Punta : Universidad de la Punta, 2023.
85 p. ; 25 x 17 cm.

ISBN 978-987-1760-83-1

1. Políticas Públicas. 2. Acceso a la Educación. 3. Educación. I. Título.
CDD 378.17344678

CC0 1.0
CC0 1.0 Universal

© Gobierno de San Luis, 2023.

Queda hecho el depósito que marca la ley 11723.
Reservados todos los derechos.
Impreso en Argentina. *Printed in Argentina*

CÉDULA DE IDENTIFICACIÓN
PROVINCIAL ELECTRÓNICA
CIPE 4.0

Universidad de LA PUNTA

MINISTERIO DE CIENCIA Y TECNOLOGÍA

GOBIERNO DE SAN LUIS

SAN LUIS NOS UNE