DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN PARA EL SERVICIO DE ENTREGA ELECTRÓNICA CERTIFICADA (DPCSCEC)

Público

Información general

Control documental

Clasificación de seguridad:	Público
Versión:	1
Fecha edición:	/11/2025
Fichero:	ENVIOGT_manual_atención_v2.r1

Estado formal

Preparado por:	Revisado por:	Aprobado por:
Nombre: Laura Paniagua Fecha: 03/11/2025	Ramón Sarante Fecha: 05 /11/2025	Francis Antonio Reyes: Fecha: 05/11/2025

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1	Original	Creación del documento	LPO	05/11/2024

Índice

1 Introducción

1.1 Presentación

Novosit, S.R.L. (el Prestador) es una entidad de certificación que Presta Servicios Cualificados de conformidad con lo establecido en la ley núm. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales. Autorizada a través de la resolución núm. 002-2021, para ofrecer:

- Generación y Emisión de Certificados Digitales Cualificados
- Generación y Emisión de Sellos Electrónicos Cualificados
- Gestión de Datos de Creación de Firmas y Sellado Cualificado
- Validación de Firmas Electrónicas, Firmas Electrónicas Avanzada y Firmas Electrónicas cualificadas.
- Sellado de Tiempo y Estampado Cronológico.
- Emisión y entrega de comunicaciones electrónicas por email y SMS.

1.2 Nombre del documento e identificación

Este documento es la "Declaración de Prácticas de Certificación del Servicio de Comunicaciones Electrónicas Certificadas" de los servicios de certificación del Prestador en lo sucesivo "DPCSCEC".

1.3 Participantes en los servicios de certificación

1.3.1 Prestador de servicios de certificación

El Prestador de Servicios Electrónicos de Certificación, en adelante "PSC" es la persona, física o jurídica, que presta uno o más servicios de certificación.

El Prestador es una entidad de certificación de conformidad, que actúa como PSC, según lo establecido en la ley núm. 126-02 sobre comercio electrónico, documentos y firmas digitales. Autorizada a través de la resolución núm. 002-2021.

1.3.2 Autoridad de registro

La Autoridad de Registro, en adelante "RA" (del término en inglés *Registry Authority*), son las personas físicas o jurídicas a las que el Prestador encomienda la identificación y verificación de la identidad de los suscriptores de los servicios de certificación.

Podrán actuar como RA del Prestador.

- La propia matriz del Prestador.
- Cualquier entidad autorizada por el Prestador.

Para poder actuar como RA será necesario formalizar contractualmente la relación existente entre el Prestador y la entidad autorizada.

Entre las funciones de estas RA, que actúan por cuenta del Prestador se encuentran:

- La comprobación de la identidad del suscriptor validando entre otras las circunstancias personales de la persona que conste como firmante del contrato.
- Verificar la información suministrada por el suscriptor en la formalización del contrato de prestación de servicios.
- Custodiar dicha información relativa a la identificación y suscripción del interesado con referencia los servicios de certificación del Prestador.
- Hacer entrega de la información necesaria para poder utilizar los servicios de certificación como pueden ser certificados, procedimientos para activar las cuentas de uso, ...

1.3.3 Autoridad de comunicaciones certificadas

La autoridad de comunicaciones certificadas, en lo sucesivo "ACC", es el tercero de confianza que presta el servicio de comunicaciones electrónicas certificadas.

El Prestador es el prestador de servicios de entrega certificada que actúa como autoridad de entrega para mensajes cuya entrega sea certificada.

1.3.4 Suscriptores del servicio de certificación

Los suscriptores son los usuarios finales de los servicios de certificación operados el Prestador. Los suscriptores del servicio pueden ser:

- Empresas, entidades, corporaciones u organizaciones que solicitan al Prestador (directamente o a través de un tercero) el uso de sus servicios en su ámbito empresarial, corporativo u organizativo.
- Las personas físicas que solicitan el servicio para sí mismas.

Los suscriptores de los servicios electrónicos de certificación son, por tanto, los clientes del PSC.

1.3.5 Partes usuarias

Las partes usuarias son las personas y las organizaciones que reciben certificados, firmas electrónicas, mensajes cuya entrega será certificada o cualquier otro de los servicios de certificación del PSC.

Como paso previo a confiar en estos mensajes, las partes usuarias deben verificarlos, como se establece en esta DPCSCEC y/o en las instrucciones disponibles en la página web del PSC.

1.3.6 Emisor y receptor

Los emisores y receptores son las cuentas de correo electrónico, pertenecientes a las partes usuarias, que emiten o reciben mensajes electrónicos cuya entrega sea certificada.

1.4 Uso de los servicios de certificación

1.4.1 Usos permitidos

El servicio de comunicaciones electrónicas certificadas genera y expide affidavits[1] con el fin de probar que una serie de datos referentes a la comunicación entre emisor y receptor han existido y no han sido alterados a partir de un instante específico en el tiempo. Su uso se limita a las aplicaciones y/o sistemas de los clientes (personas físicas o jurídicas) que han contratado estos servicios.

1.4.2 Límites y prohibiciones de uso

El servicio de comunicaciones electrónicas certificadas no se utilizará para fines distintos de los especificados en el presente documento. Del mismo modo, el servicio deberá emplearse únicamente de acuerdo con la regulación aplicable.

1.5 Administración de la política

1.5.1 Organización que administra el documento

Los datos de la sociedad son los siguiente:

- Novosit, Sociedad de Responsabilidad Limitada (SRL)
- RNC: 1-30-38057-2
- Registro Mercantil: 50537SD.

Comentado [LEPO1]: Confirmar que la información en correcta, hemos colocado los de la página web y la anterior DPC.

1.5.2 Datos de contacto de la organización

Los datos de contacto del Prestador., son los siguientes:

- Web: https://www.novosit.com.
- Email: info@novosit.com
- Teléfono: 809-440-7964
- Domicilio Empresa: Avenida Pedro A. Bobea, esq. Anacaona, edif. Curvo, apto. 495, Bella Vista, Santo Domingo. D.N.

1.5.3 Procedimientos de gestión del documento

El sistema documental y de organización del Prestador garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de este documento y de las especificaciones de servicio relacionados con el mismo.

[1] *Affidavit*: documento legal que sirve como testimonio o declaración jurada ante un tribunal, o como garantía o aval en otros casos. © Diccionario panhispánico del español jurídico.

2 Publicación y preservación

2.1 Depósito

El Prestador custodia de manera segura todos los *affidavits* generados un mínimo de 15 años. Asimismo, dispone de un Depósito, en el que se publican las informaciones relativas al servicio de comunicaciones electrónicas certificadas. El Depósito se puede consultar en https://www.novosit.com/.

Dicho servicio se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control del Prestador, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo de acuerdo con los plazos y procedimientos establecidos con respecto de la continuidad del negocio.

2.2 Publicación de información del prestador de servicios de certificación

El Prestador publicará las siguientes informaciones, en su depósito:

- La Declaración de Prácticas de Certificación del Servicio de Comunicaciones Certificadas (DPCSCEC).
- Las listas de certificados revocados.
- Las claves públicas de los certificados utilizados para la entrega certificada.
- Con carácter previo, y siempre que sea posible, cualquier información que afecte a los participantes en los servicios de certificación.

2.3 Frecuencia de publicación

La información del PSC, incluyendo la DPCSCEC, se publica en cuanto se encuentra disponible.

Los cambios en la DPCSCEC se rigen por lo establecido en el procedimiento de gestión de este documento y de acuerdo con la normativa de aplicación.

2.4 Control de acceso

El Prestador no limita el acceso de lectura a las informaciones establecidas en la sección “Publicación de información del prestador de servicios de certificación”, pero establece controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del Depósito, para proteger la integridad y autenticidad de la información.

El Prestador emplea sistemas fiables para el depósito, de modo tal que:

- Únicamente las personas autorizadas pueden hacer anotaciones y modificaciones.
- Puede comprobarse la autenticidad de la información.

- Puede detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

3 Autenticación

3.1 Autenticación del emisor

La autenticación del emisor para enviar comunicaciones se hará mediante usuario (vinculando a su correo electrónico) y contraseña, proveyendo el servicio, medios para aplicar políticas complejas de contraseñas y cambios seguros de las mismas.

3.2 Autenticación del receptor

La autenticación del receptor se realiza mediante doble factor de autenticación con una URL temporal aleatoria, y la posibilidad de incluir un OTP (*One-Time Password*) que será enviado al email o teléfono móvil del receptor.

4 Requisitos operacionales

4.1 Acceso al servicio

El acceso a las diferentes URL del servicio siempre se realizará mediante protocolos seguros y comunicaciones cifradas.

4.2 Eventos y evidencias

El servicio del Prestador permite recopilar evidencias que permitan asegurar que los mensajes electrónicos del emisor son entregados al receptor de estos garantizando la integridad de la evidencia y la veracidad de esta.

El encargado de garantizar esta integridad y veracidad es el propio PSC, a través de una serie de procesos criptográficos como la aplicación de firmas electrónicas y sellos de tiempo. Tanto los procesos de firma como los sellos de tiempo son proporcionados por PSC.

Las evidencias en este servicio se denominan *affidavits* y son documentos en los que se recopila toda la información pericial que permita demostrar que un evento se ha producido, y no ha sido modificado con posterioridad. En los *affidavits* se puede encontrar:

- Datos de información del emisor y receptor de los mensajes electrónicos.
- El contenido emitido, junto con los documentos adjuntos procesados, además se incorporan resúmenes criptográficos de los mismos.
- En los *affidavits* se puede encontrar información sobre los siguientes eventos:
    - Envío y emisión al servidor de correo del destinatario.
    - Entrega al servidor de correo del destinatario o fallo si no se pudiera entregar.
    - Apertura del mensaje.

- O acciones posteriores del receptor (si es que se producen).
- La referencia temporal estará indicada en horario *Coordinated Universal Time* (UTC).

Cada *affidavit* es firmado electrónicamente por el servicio, y se le puede añadir un sello de tiempo, para de esta manera garantizar la integridad del documento y que éste no haya sido modificado con posterioridad.

El emisor tendrá acceso a todos sus *affidavits* en el servicio de comunicaciones electrónicas certificadas, durante el periodo de custodia contratado con un periodo mínimo de quince años. El receptor podrá acceder a los *affidavits* a través del servicio de soporte o por información del emisor. Una vez que el periodo de vigencia contratado haya concluido ninguna de las partes tendrá acceso a los *affidavits*.

En el caso de producirse un fallo con la integridad de los *affidavits*, o se produjera cualquier incidencia asociada a la integridad del contenido durante el proceso de entrega se comunicará desde el servicio de soporte del Prestador a las partes interesadas.

5 Controles de seguridad física, de gestión y de operaciones

5.1 Controles de seguridad física

El Prestador ha establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones para la prestación de los servicios electrónicos de certificación.

En concreto, la política de seguridad del Prestador aplicable a los servicios electrónicos de certificación establece prescripciones sobre lo siguiente:

- Controles de acceso físico.
- Protección frente a desastres naturales.
- Medidas de protección frente a incendios.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Protección antirrobo.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.

Estas medidas resultan aplicables a las instalaciones desde donde se prestan los servicios electrónicos de certificación, en sus entornos de producción y contingencia, las cuales son auditadas periódicamente de acuerdo con la normativa aplicable y a las políticas propias del Prestador destinadas a este fin.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia las 24 horas siguientes al aviso.

5.2 Localización y construcción de las instalaciones

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta y está ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.

La sala donde se realizan las operaciones criptográficas en el Centro de Proceso de Datos principal cuenta con redundancia en sus infraestructuras, así como varias fuentes alternativas de electricidad y refrigeración en caso de emergencia.

El Prestador dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de estos.

5.2.1 Acceso físico

El Prestador dispone de tres niveles de seguridad física en el CPD principal (entrada del Edificio donde se ubica, acceso a la sala del CPD y acceso al Rack), debiendo accederse desde los niveles inferiores a los niveles superiores.

El acceso físico a las dependencias del Prestador donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales. Así:

- Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro de este.
- El acceso a las salas se realiza con lectores de tarjeta de identificación y/o cerraduras electrónicas, gestionado por un sistema informático que mantiene un log de entradas y salidas automático.
- Para el acceso a la sala donde se ubican los procesos criptográficos es necesario la autorización previa del Prestador a los administradores del servicio de *colocation* que disponen de la llave para abrir la sala y la jaula, pero no los armarios.

5.2.2 Electricidad y aire acondicionado

Las instalaciones del CPD principal del Prestador disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado con un grupo electrógeno.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado.

5.2.3 Exposición al agua

Las instalaciones están ubicadas en una zona de bajo riesgo de inundación. Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

5.2.4 Prevención y protección de incendios

Las instalaciones y activos del CPD principal del Prestador cuentan con sistemas automáticos de detección y extinción de incendios.

5.2.5 Almacenamiento de soportes

Únicamente el personal autorizado tiene acceso a los medios de almacenamiento. La información de más alto nivel de clasificación se guarda en una caja de seguridad fuera de las instalaciones del Centro de Proceso de Datos principal.

5.2.6 Tratamiento de residuos

La eliminación de soportes, tanto papel como magnéticos, se realizan mediante mecanismos que garantizan la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se desechan en cuyo caso se destruyen físicamente, o se reutilizan previo proceso de borrado permanente o formateo. En el caso de documentación en papel, mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

5.2.7 Copia de respaldo fuera de las instalaciones

El Prestador utiliza un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos que son independientes del Centro de Proceso de Datos principal.

5.3 Controles de procedimientos

El Prestador garantiza que sus sistemas se operan de forma segura, para lo cual ha establecido e implantado procedimientos para las funciones que afectan a la provisión de sus servicios.

El personal al servicio del Prestador ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

5.3.1 Funciones fiables

El Prestador ha identificado, de acuerdo con su política de seguridad, las siguientes funciones o roles con la condición de fiables:

- **Administrador de Sistemas**: responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación
- **Auditor Interno**: responsable de proporcionar aseguramiento del cumplimiento de los procedimientos operativos por parte de sus responsables. Se trata de una persona externa al departamento de Sistemas de Información. Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.

- **Custodio**: responsable de custodiar las tarjetas criptográficas donde se almacena la clave precompartida bajo el modelo de seguridad n de m. Esta función es compatible con el resto de las funciones de esta DPCSCEC.
- **Oficial de verificación de identidad**: responsable de asegurar los procesos de verificación de la identidad de los suscriptores de alguno de los servicios de certificación del Prestador.
- **Operador de Sistemas**: responsable necesario juntamente con el Administrador de Sistemas del funcionamiento correcto del hardware y software soporte de la plataforma de certificación. El operador es responsable de los procedimientos de copia de respaldo y mantenimiento de las operaciones diarias de los sistemas.
- **Propietario de producto**: encargado de coordinar, controlar y gestionar los equipos y entregables de los desarrollos del Prestador. Debe encargarse de las tareas de triaje de errores y funcionalidades, y será el responsable de desplegarlos en los diferentes entornos.
- **Responsable de Seguridad**: encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad del Prestador. Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos. Adicionalmente, el Prestador implementa criterios en sus políticas para la segregación de las funciones, como medida de prevención de actividades fraudulentas.

5.3.2 Identificación y autenticación para cada función

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurará que cada persona realiza las operaciones para las que está asignado.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante usuario/contraseña, certificado digital, tarjeta de acceso físico y/o llaves.

5.3.3 Roles que requieren separación de tareas

Las funciones fiables se establecen bajo el principio del mínimo privilegio, garantizado una segregación de funciones, de modo que la persona que ostente un rol no tenga un control total o especialmente amplio de todas las funciones de certificación, asegurando el debido control y vigilancia, limitando así cualquier tipo de comportamiento fraudulento a nivel interno.

La concesión del mínimo privilegio para las funciones de confianza, se hará teniendo en cuenta el mejor desarrollo de la actividad y será lo más limitado posible, considerando la estructura organizativa del Prestador en cada momento.

5.4 Controles de personal

5.4.1 Requisitos de historial, calificaciones, experiencia y autorización

Todo el personal está cualificado y/o ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

El personal en puestos de confianza no tiene intereses personales que entren en conflicto con el desarrollo de la función que tenga encomendada.

En general, el Prestador retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de conflictos de interés y/o la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.

El Prestador no asignará un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por una falta que afecte su idoneidad para el puesto. Por este motivo, previamente se realiza una investigación hasta donde permita la legislación aplicable, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales.
- Referencias profesionales.

5.4.2 Procedimientos de investigación de historial

El Prestador, antes de contratar a una persona o de que ésta acceda al puesto de trabajo, realiza las siguientes comprobaciones:

- Referencias de los trabajos de los últimos años
- Referencias profesionales
- Estudios, incluyendo titulación alegada.

El Prestador obtiene el consentimiento inequívoco del afectado para dicha investigación previa, y procesa y protege todos sus datos personales en cumplimiento de la normativa vigente en materia de protección de datos personales.

Todas las comprobaciones se realizan hasta donde lo permite la legislación vigente aplicable. Los motivos que pueden dar lugar a rechazar al candidato a un puesto fiable son los siguientes:

- Falsedades en la solicitud de trabajo, realizadas por el candidato.
- Referencias profesionales muy negativas o muy poco fiables en relación con el candidato.

5.4.3 Requisitos de formación

El Prestador forma al personal en puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, manteniendo archivo de dicha formación.

Los programas de formación son revisados periódicamente, y son actualizados de forma periódica.

La formación incluye, al menos, los siguientes contenidos:

- Tareas que debe realizar la persona.
- Políticas y procedimientos de seguridad del Prestador. Uso y operación de maquinaria y aplicaciones instaladas.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

5.4.4 Requisitos y frecuencia de actualización formativa

El Prestador, actualiza la formación del personal de acuerdo con las necesidades, y con la frecuencia suficiente para cumplir sus funciones de forma competente y satisfactoria, especialmente cuando se realicen modificaciones sustanciales en las tareas de certificación.

5.4.5 Secuencia y frecuencia de rotación laboral

N/A

5.4.6 Sanciones para acciones no autorizadas

El Prestador dispone de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, adecuado a la legislación laboral aplicable.

Las acciones disciplinarias incluyen la suspensión, separación de las funciones y hasta el despido de la persona responsable de la acción dañina, de forma proporcionada a la gravedad de la acción no autorizada.

5.4.7 Requisitos de contratación de profesionales

Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados el Prestador. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían, una vez evaluados, dar lugar al cese del contrato laboral.

En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la DPCSCEC, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, no obstante, lo cual, el PSC será responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por tercero distinto al Prestador.

5.4.8 Suministro de documentación al personal

El prestador de servicios de certificación suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de realizar su trabajo de forma competente y satisfactoria.

5.5 Procedimientos de auditoría de seguridad

5.5.1 Tipos de eventos registrados

El Prestador produce y guarda registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados a los sistemas que dan soporte a los servicios de certificación a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones.
- Encendido y apagado de las aplicaciones de los servicios de certificación.
- Cambios en los detalles de los servicios de certificación y/o sus claves.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de éste.
- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor, en caso de certificados individuales, o de la persona física identificada en el certificado, en caso de certificados de organización.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte al servicio.
- Eventos relativos a la sincronización y recalibración del reloj.

Las entradas del registro incluyen los siguientes elementos:

- Fecha y hora de la entrada.
- Número de serie o secuencia de la entrada, en los registros automáticos.
- Identidad de la entidad que entra el registro.
- Tipo de entrada.

5.5.2 Frecuencia de tratamiento de registros de auditoría

El Prestador revisa sus logs cuando se produce una alerta del sistema motivada por la existencia de algún incidente.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas.

El Prestador mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de logs.
- Que los ficheros de logs no se reescriben.
- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.
- Los ficheros de logs se guardarán en ficheros estructurados susceptibles de incorporarse en una BBDD para su posterior exploración.

5.5.3 Período de conservación de registros de auditoría

El Prestador almacena la información de los logs durante un periodo de entre 1 y 20 años, en función del tipo de información registrada.

5.5.4 Protección de los registros de auditoría

Los ficheros de registro de auditoría se protegen mediante controles físicos y lógicos de acceso, lecturas, modificaciones, borrados no autorizados.

El acceso a los ficheros de logs está reservado sólo a las personas autorizadas. Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de logs de auditoría.

5.5.5 Procedimientos de copia de respaldo

El Prestador dispone de un procedimiento adecuado de copia de seguridad de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

5.5.6 Localización del sistema de acumulación de registros de auditoría

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo, las comunicaciones de red y por el software de los servicios de certificación, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado. Todo ello compone el sistema de acumulación de registros de auditoría.

5.5.7 Notificación del evento de auditoría al causante del evento

Cuando el sistema de acumulación de registros de auditoría registra un evento, no es preciso enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

5.5.8 Análisis de vulnerabilidades

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría del Prestador.

Los análisis de vulnerabilidad deben ser ejecutados, repasados y revisados por medio de un examen de estos acontecimientos monitorizados. Estos análisis deben ser ejecutados periódicamente de acuerdo con el procedimiento interno que está previsto para este fin.

Los datos de auditoría de los sistemas son almacenados con el fin de ser utilizados en la investigación de cualquier incidencia y localizar vulnerabilidades.

5.6 Archivos de informaciones

5.6.1 Período de conservación de registros

El Prestador archiva los registros especificados anteriormente durante al menos 15 años, o el período que establezca la legislación vigente.

El archivo de información estará disponible para su consulta por un auditor cualificado en función del cumplimiento de la legislación vigente.

5.6.2 Protección del archivo

El Prestador protege el archivo de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo. El archivo está protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable.

El Prestador asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en instalaciones seguras externas.

5.6.3 Procedimientos de copia de respaldo

El Prestador dispone de un centro de almacenamiento externo del CPD principal para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido sólo para personal autorizado.

El Prestador como mínimo realiza copias de respaldo diarias de todos sus documentos electrónicos para casos de recuperación de datos.

5.6.4 Requisitos de sellado de fecha y hora

Los registros están fechados con una fuente fiable vía NTP. No es necesario que esta información se encuentre firmada digitalmente.

5.6.5 Localización del sistema de archivo

El Prestador dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

5.6.6 Procedimientos de obtención y verificación de información de archivo

El Prestador dispone de un procedimiento donde se describe el proceso para verificar que la información archivada es correcta y accesible. El Prestador proporciona la información y medios de verificación al auditor.

5.7 Renovación de claves

Las claves y certificados de los servicios de certificación están únicamente asociadas con el sistema que presta dicho servicio. Con anterioridad al uso de las claves privadas de los servicios de certificación, se realizará un cambio de claves o revocación de las actuales.

5.8 Compromiso de claves y recuperación de desastre

5.8.1 Procedimientos de gestión de incidencias y compromisos

El Prestador ha desarrollado políticas de seguridad y continuidad del negocio que le permiten la gestión y recuperación de los sistemas en caso de incidentes y compromiso de sus operaciones.

5.8.2 Corrupción de recursos, aplicaciones o datos

Cuando acontezca un evento de corrupción de recursos, aplicaciones o datos, se seguirán los procedimientos de gestión oportunos de acuerdo con las políticas de seguridad y gestión de incidentes del Prestador, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se iniciarán los procedimientos de compromiso de claves o de recuperación de desastres del Prestador.

5.8.3 Compromiso de las claves privadas de la entidad

En caso de sospecha o conocimiento del compromiso del Prestador, se activarán los procedimientos de compromiso de claves de acuerdo con las políticas de seguridad, gestión de incidencias y continuidad del negocio, que permita la recuperación de los sistemas críticos, si fuera necesario en un centro de datos alternativo.

5.8.4 Continuidad del negocio después de un desastre

El Prestador restablecerá los servicios críticos de acuerdo con el plan de incidencias y continuidad de negocio existente restaurando la operación normal de los servicios anteriores en las 24 horas siguientes al desastre.

5.9 Terminación del servicio

El Prestador asegura que las posibles interrupciones a los suscriptores de los servicios y a terceras partes son mínimas como consecuencia del cese de los servicios del prestador de servicios de

certificación. En este sentido, el Prestador garantiza un mantenimiento continuo de los registros definidos y por el tiempo establecido de acuerdo con la presente DPCSCEC.

No obstante, lo anterior, si procede el Prestador ejecutará todas las acciones que sean necesarias para transferir a un tercero o a un depósito notarial, las obligaciones de mantenimiento de los registros especificados durante el periodo correspondiente según esta DPCSCEC o la previsión legal que corresponda.

Antes de terminar sus servicios, el Prestador desarrolla un plan de terminación, con las siguientes provisiones:

- Proveerá de los fondos necesarios, incluyendo un seguro de responsabilidad civil, para continuar la finalización de las actividades de revocación.
- Informará a todos Suscriptores del servicio, Tercero que confían y en general cualquier tercero con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 2 meses.
- Transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios.
- Destruirá o deshabilitará para su uso las claves privadas encargadas de los servicios de certificación.
- Ejecutará las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de eventos durante los períodos de tiempo respectivos.
- Comunicará al Órgano Supervisor correspondiente, con una antelación mínima de 2 meses, el cese de su actividad.
- Asimismo, le comunicará la apertura de cualquier proceso concursal que se siga contra el Prestador, así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.

6 Controles de seguridad técnica

El Prestador emplea sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

Los certificados electrónicos cualificados del servicio de comunicaciones electrónicas certificadas serán generados por Prestadores de Servicios Cualificados, de acuerdo con su Declaración de Prácticas de Certificación, encontrándose disponibles en su página web.

Asimismo, se han seguido los procedimientos de ceremonia de claves, dentro del perímetro de alta seguridad destinado a esta tarea. Las actividades realizadas durante la ceremonia de generación de claves han sido registradas, fechadas y firmadas por todos los individuos participantes en la misma.

Dichos registros son custodiados a efectos de auditoría y seguimiento durante un período apropiado determinado por el Prestador.

Para la generación de claves de los certificados electrónicos del servicio de comunicaciones electrónicas certificadas se utilizan dispositivos con las certificaciones *Common Criteria EAL4+*.

Las claves son generadas usando el algoritmo de clave pública RSA, con una longitud mínima de 2048 bits.

Certificados electrónicos cualificados	2.048 bits	Hasta 5 años

6.1.2 Envío de la clave pública al emisor del certificado

Los métodos para la remisión de la clave pública al prestador de servicios electrónicos de certificación es *PKCS#10*, otra prueba criptográfica equivalente o cualquier otro método aprobado por el Prestador.

6.1.3 Distribución de la clave pública del prestador de servicios de certificación

Las claves públicas son comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen, mediante su publicación en el Depósito.

Los usuarios pueden acceder al Depósito para obtener las claves públicas, y adicionalmente, en aplicaciones S/MIME, el mensaje de datos puede contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

El certificado de las autoridades de certificación raíz y subordinadas estarán a disposición de los usuarios en sus propias páginas web.

6.1.4 Tamaños de claves

La longitud de las claves de los certificados utilizados para la firma de los *affidavits* será como mínimo de 2048 bits.

6.1.5 Generación de parámetros de clave pública

La clave pública de los certificados utilizados para la firma de los *affidavits* está codificada preferentemente de acuerdo con RFC 5280.

6.1.6 Comprobación de calidad de parámetros de clave pública

La calidad de los parámetros de la clave pública será por lo menos:

- Longitud del Módulo = 4096 bits
- Algoritmo de generación de claves: rsagen1
- Funciones criptográficas de Resumen: SHA256.

6.1.7 Generación de claves en aplicaciones informáticas o en bienes de equipo

Todas las claves se generan en bienes de equipo, de acuerdo con lo indicado en el apartado "Generación del par de claves".

6.2 Protección de las claves privadas

6.2.1 Estándares de módulos criptográficos

Los módulos que gestionan claves del Prestador cumplen con la certificación *Common Criteria EAL4+* o equivalente.

6.2.2 Control sobre las claves privada

La gestión de acceso a las claves privadas de los certificados de los servicios de certificación se realiza según los controles establecidos por el HSM donde se custodian. Asimismo, los dispositivos criptográficos se encuentran protegidos físicamente tal y como se determina en este documento.

6.2.3 Copia de respaldo de las claves privada

El Prestador realiza copias de backup de las claves privadas de los certificados, de tal manera que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de estas. Tanto la generación de la copia como la recuperación de ésta necesitan al menos de la participación de dos personas.

Estos ficheros de recuperación se almacenan en armarios ignífugos y en el centro de custodia alternativo.

6.2.4 Introducción de las claves privadas en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos de producción del Prestador donde se almacenan cifradas.

6.2.5 Método de activación de las claves privada

Las claves privadas del Prestador se activan mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico.

6.2.6 Método de desactivación de las claves privada

Para la desactivación de las claves privadas del Prestador se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente.

6.2.7 Método de destrucción de las claves privada

Para la destrucción de las claves privadas se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente.

Con anterioridad a la destrucción de las claves, se emitirá una revocación del certificado de las claves públicas asociadas a las mismas.

- Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas del Prestador. Para el reinicio se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.
- Finalmente se destruirán de forma segura las copias de seguridad.

6.3 Controles de seguridad informática

El Prestador emplea sistemas fiables para ofrecer sus servicios de certificación. El Prestador ha realizado controles y auditorías informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Respecto a la seguridad de la información, el Prestador aplica los controles del esquema de certificación sobre sistemas de gestión de la información ISO 27001.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas del Prestador, en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.
- Configuración de Usuarios y permisos.
- Configuración de eventos de Log.
- Plan de backup y recuperación.
- Requerimientos de tráfico de red.

Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

6.4 Controles técnicos del ciclo de vida

6.4.1 Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas por el Prestador de acuerdo con estándares de desarrollo y control de cambios.

Las aplicaciones disponen de métodos para la verificación de la integridad y autenticidad, así como de la corrección de la versión a emplear.

6.4.2 Controles de gestión de seguridad

El Prestador desarrolla actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un grupo para la gestión de la seguridad. En la realización de esta función dispone de un plan de formación anual.

El Prestador exige medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de servicios electrónicos de certificación.

6.4.2.1 Clasificación y gestión de información y bienes

El Prestador mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

La política de seguridad del Prestador detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: PÚBLICO, USO INTERNO y CONFIDENCIAL.

6.4.2.2 Operaciones de gestión

El Prestador dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos.

En el documento de seguridad del Prestador se desarrolla en detalle el proceso de gestión de incidencias.

El Prestador tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

6.4.2.3 Tratamiento de los soportes y seguridad

Todos los soportes son tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

6.4.2.4 Planificación del sistema

El departamento de atención al cliente del Prestador mantiene un registro de las capacidades de los equipos. Juntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

6.4.2.5 Reportes de incidencias y respuesta

El Prestador dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación del proceso de resolución de la incidencia.

6.4.2.6 Procedimientos operacionales y responsabilidades

El Prestador define actividades, asignadas a personas con un rol de confianza, distintas de las actividades asignadas a personas que no tienen ese rol. Dichas actividades no tienen carácter confidencial.

6.4.2.7 Gestión del sistema de acceso

El Prestador realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.

En particular:

- Se dispone de controles basados en firewalls en alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.
- El Prestador dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- El Prestador dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.
- Cada persona tiene asociado un rol para realizar las operaciones de certificación.
- El personal del Prestador es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

6.4.2.8 Gestión del ciclo de vida del hardware criptográfico

El Prestador asegura que el hardware criptográfico usado para la firma de certificados o los servicios de certificación no se manipula durante su transporte mediante la inspección del material entregado.

En particular:

- El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación.
- El Prestador registra toda la información pertinente del dispositivo para añadir al catálogo de activos.
- El uso del hardware criptográfico requiere de al menos dos empleados de confianza.
- El Prestador realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.
- El dispositivo hardware criptográfico solo es manipulado por personal confiable.
- Las claves privadas de los certificados del Prestador almacenadas en el hardware criptográfico se eliminarán una vez se haya retirado el dispositivo.
- La configuración del sistema del Prestador, así como sus modificaciones y actualizaciones son documentadas y controladas.
- Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

6.5 Controles de seguridad de red

El Prestador protege el acceso físico a los dispositivos de gestión de red, y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad, creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se transfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos TLS o del sistema VPN con autenticación por doble factor.

6.6 Controles de ingeniería de módulos criptográficos

Los módulos criptográficos se someten a los controles de ingeniería previstos en las normas indicadas a lo largo de esta sección.

Los algoritmos de generación de claves empleados se aceptan comúnmente para el uso de la clave a la que están destinados.

Todas las operaciones criptográficas del Prestador son realizadas en módulos con la certificación *Common Criterial 4 EAL+* o equivalentes.

6.7 Fuentes de Tiempo

Todos los dispositivos utilizados por el Prestador están sincronizados mediante protocolo NTP (*Network Time Protocol*) a través de internet (*RFC 1305 Network Time Protocol*), utilizando alguno de los siguientes servidores *NTP stratum 1*, como pueden ser el Real Observatorio de la Armada, RedIris o los *pooles* de servidores de tiempo del proyecto NTP (http://www.ntp.org/).

7 Perfiles de certificados y revocación de estos

La información sobre los perfiles de los certificados emitidos o utilizados por el Prestador se indica en su correspondiente declaración de prácticas y política de cada perfil de certificados, o de los servicios de certificación.

8 Auditoría de conformidad

El Prestador ha comunicado el inicio de su actividad como prestador de servicios de certificación por el Órgano Supervisor, y se encuentra sometida a las revisiones de control que este organismo considere necesarias.

8.1 Frecuencia de la auditoría de conformidad

El Prestador lleva a cabo una auditoría de conformidad anualmente, además de las auditorías internas que realiza bajo su propio criterio o en cualquier momento, debido a una sospecha de incumplimiento de alguna medida de seguridad.

8.2 Identificación y calificación del auditor

Las auditorías son realizadas por una firma de auditoría independiente externa que demuestra competencia técnica y experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación de clave pública, y los elementos relacionados.

8.2.1 Relación del auditor con la entidad auditada

Las empresas de auditoría son de reconocido prestigio con departamentos especializados en la realización de auditorías informáticas, por lo que no existe ningún conflicto de intereses que pueda desvirtuar su actuación en relación con el Prestador.

8.3 Listado de elementos objeto de auditoría

La auditoría verifica respecto al Prestador:

- Que la entidad tiene un sistema de gestión que garantice la calidad del servicio prestado.
- Que la entidad cumple con los requerimientos de la DPCSCEC y otra documentación vinculada con la emisión de los distintos certificados digitales.
- Que la DPCSCEC y demás documentación jurídica vinculada, se ajusta a lo acordado por el Prestador y con lo establecido en la normativa vigente.
- Que la entidad gestiona de forma adecuada sus sistemas de información

8.4 Acciones que emprender como resultado de una falta de conformidad

Una vez recibido por la dirección el informe de la auditoría de cumplimiento realizada, se analizan, con la firma que ha ejecutado la auditoría, las deficiencias encontradas y desarrolla y ejecuta las medidas correctivas que solucionen dichas deficiencias.

Si el Prestador es incapaz de desarrollar y/o ejecutar las medidas correctivas o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema, deberá comunicarlo inmediatamente al Comité de Dirección del Prestador que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.
- Solicitar la revocación de las claves de los certificados de los servicios de certificación y regenerar la infraestructura.
- Terminar el servicio de certificación afectado.
- Otras acciones complementarias que resulten necesarias.

8.5 Tratamiento de los informes de auditoría

Los informes de resultados de auditoría se entregan al Comité de Dirección del Prestador en un plazo máximo de 15 días tras la ejecución de la auditoría.

9 Requisitos comerciales y legales

9.1 Tarifas

9.1.1 Tarifa de los servicios de certificación

El Prestador puede establecer una tarifa por el uso de sus servicios de certificación, de la que, en su caso, se informará oportunamente a los suscriptores.

9.1.2 Política de reintegro

Sin estipulación.

9.2 Capacidad financiera

El Prestador dispone de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios, según lo establecido en la ETSI EN 319 401-1 7.12 y la normativa nacional aplicable con relación a la gestión de la finalización de los servicios y plan de cese.

9.2.1 Cobertura de seguro

El Prestador dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional, que mantiene de acuerdo con la normativa vigente aplicable.

9.2.2 Otros activos

Sin estipulación.

9.2.3 Cobertura de seguro para suscriptores y terceros que confían en los servicios de certificación

La Entidad de Certificación contará con seguros vigentes acordes con las responsabilidades asumidas, que cumplan con los requisitos establecidos por INDOTEL.

9.3 Confidencialidad

9.3.1 Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales el Prestador:

- Las solicitudes del servicio, así como toda otra información personal obtenida para la prestación de este, excepto las informaciones indicadas en la sección siguiente.

- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa.
- Planes de continuidad de negocio y de emergencia.
- Planes de seguridad.
- Documentación de operaciones, archivo, monitorización y otros análogos.
- Toda otra información identificada como “Confidencial”.

9.3.2 Divulgación legal de información

El Prestador no divulgará la información confidencial excepto en los casos legalmente previstos.

9.4 Protección de datos personales

El Prestador garantiza el cumplimiento de la normativa vigente en materia de protección de datos personales, reflejada en la Ley núm. 172-13, sobre Protección de Datos Personales, la Resolución núm. 55-06 que aprueba la norma complementaria de la ley 126-02 sobre Protección de Datos de Carácter Personal por los Sujetos Regulados y en general cualquier normativa nacional que resulte de aplicación.

En cumplimiento de esta, el Prestador ha documentado en esta DPCSCEC los aspectos y procedimientos de seguridad y organizativos, con el fin de garantizar que todos los datos personales a los que tenga acceso son protegidos ante su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado.

A continuación, se detalla toda la información necesaria con respecto al tratamiento de datos personales realizado el Prestador:

9.4.1 Responsable del tratamiento

El responsable del tratamiento de datos de carácter personal va a ser:

- Novosit, S.R.L.
- RNC: 1-30-38057-2
- Registro Mercantil: 50537SD.
- Web: https://www.novosit.com.
- Email: info@novosit.com
- Teléfono: 809-482-6787
- Fax: 809-482-5434
- Domicilio Empresa: Av. Pedro A. Bobea, esq. Anacaona, edif. curvo, apto. 495, Bella Vista, Santo Domingo. D.N.

9.4.2 Datos de contacto de la organización

Los datos de contacto del delegado de protección de datos son:

- Web: https://www.novosit.com.

- Email: info@novosit.com
- Teléfono: 809-482-6787
- Fax: 809-482-5434
- Domicilio Empresa: Av. Pedro A. Bobea, esq. Anacaona, edif. curvo, apto. 495, Bella Vista, Santo Domingo. D.N.
-

9.4.3 Finalidades del tratamiento

El Prestador tiene el deber de informar a los usuarios, que todos sus datos de carácter personal facilitados se tratan para las siguientes finalidades:

- **Prestación de Servicios electrónicos de certificación**. Los datos son recabados mediante el contrato oportuno y son tratados con la finalidad de llevar a cabo los servicios electrónicos solicitados y contratados por los usuarios, todo ello en base a lo establecido en la presente DPCSCEC.
    - Certificación de procesos de comunicación, incluyendo (i) la certificación del contenido comunicado (que puede incluir datos personales) mediante mecanismos criptográficos de comprobación de la integridad, (ii) la certificación de las direcciones o teléfonos del emisor y del receptor y (iii) la certificación del proceso de entrega y/o apertura.
    - Certificación de procesos de consentimiento: servicios para la visualización segura del contenido (que puede incluir datos personales) y/o la firma de este mediante algún mecanismo de identificación y autenticación.
    - Custodia de evidencias: (i) conservación del contenido a largo plazo, as√≠ como las evidencias relacionadas con los procesos de certificación (affidavits e historial de eventos) y (ii) provisión de servicios de búsqueda y consulta, incluyendo la capacidad de búsqueda por dirección del destinatario o firmante (cuando aplique).
    - En este supuesto, el Prestador actúa como encargado del tratamiento, siendo el responsable la entidad que le remite la comunicación. La finalidad es la gestión de la comunicación que se le remite.
- **Soporte para la prestación de los servicios**. Mantenimiento de datos de contacto para facilitar la gestión de peticiones e incidencias relacionadas con la prestación de los Servicios. Por ejemplo, el CLIENTE o directamente el Usuario, puede facilitar sus datos de contacto, para intentar resolver una incidencia relacionada con problemas en los servicios ofertados el Prestador.
- **Relación mercantil**. Mantenimiento de datos de contacto de empleados del CLIENTE para facilitar la gestión comercial, facturación, seguimiento y gestión de los Servicios.

El Prestador informa que los datos personales facilitados únicamente se tratarán para las finalidades anteriormente descritas y no serán tratados de manera incompatible con las mismas.

9.4.4 Legitimación del tratamiento

De acuerdo con las finalidades de tratamiento indicadas, la base legal para el tratamiento de los datos personales de los usuarios es:

- La legitimación del tratamiento para la Prestación de Servicios electrónicos de certificación es la ejecución del contrato de los servicios solicitados, donde el usuario es parte de este, el cual presta expresa e inequívocamente, mediante acción positiva y previa al uso del servicio, al aceptar las condiciones.
- La legitimación del tratamiento para atender las consultas y solicitudes se basa en el interés legítimo, por ejemplo, para atender al destinatario de una comunicación o para validar un documento firmado, resultado de la prestación de los servicios.

El consentimiento para el tratamiento puede ser retirado en cualquier momento mediante una solicitud en https://www.el Prestador.com o por correo electrónico a la dirección email especificada en el apartado Datos de contacto de la organización.

El usuario garantiza que los datos aportados son verdaderos, exactos, completos y actualizados, siendo responsable de cualquier daño o perjuicio, directo o indirecto, que pudiera ocasionarse como consecuencia del incumplimiento de tal obligación.

9.4.5 Datos tratados y conservación

Las categorías de datos personales tratados el Prestador, a título enunciativo, pero no limitativo, comprenden datos identificativos (nombre, apellidos y los propios de identidad) y datos de contacto (dirección postal, correo electrónico y teléfono), y algún dato adicional como la dirección IP, datos del navegador y datos de trazabilidad.

Los datos personales se conservarán mientras sean necesarios para dar respuesta a las consultas y solicitudes, hasta la finalización de la relación contractual y posteriormente, durante los plazos legalmente exigidos acorde a cada caso, tal y como se encuentran definidos en la presente DPCSCEC. En caso de imperativo legal, ésta permanecerá bloqueada, exclusivamente a disposición de jueces y tribunales, los periodos de tiempo legalmente establecidos.

9.4.6 Cesión y transferencia internacional de datos

Los datos personales no se divulgan ni se ceden a terceros salvo:

- Obligación legal

- Interés legítimo sobre los datos, como puede ser, el destinatario de las comunicaciones o los firmantes de los documentos, objeto de los Servicios electrónicos de certificación, que contengan dichos datos
- Para atender un requerimiento judicial o de cualquier autoridad administrativa competente que así lo requiera
- Terminación de los servicios

Se realizarán transferencias internacionales a la Unión Europea o al Espacio Económico Europeo (EEE).

9.4.7 Derechos de los usuarios

- **Confirmación**. Todos los usuarios tienen derecho a obtener confirmación sobre si el Prestador está tratando datos personales que les concierne.
- **Acceso y rectificación**. Los usuarios tienen derecho a acceder a todos sus datos personales, así como solicitar la rectificación de aquellos que sean inexactos o erróneos.
- Supresión / cancelación. Los usuarios podrán solicitar la supresión/cancelación de los datos cuando, entre otros motivos, éstos no sean necesarios para los fines para los que fueron recogidos.
- **Limitación y oposición**. El usuario podrá solicitar la limitación del tratamiento para que sus datos personales no se apliquen en las operaciones que correspondan. En determinadas circunstancias y por motivos relacionados con su situación particular, el usuario podrá oponerse al tratamiento de datos, estando el Prestador obligada a dejar de tratarlos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones.
- **Portabilidad**. Los interesados podrán solicitar que sus datos personales les sean enviados o bien se transmitan a otro responsable, en un formato electrónico estructurado y de uso habitual.

Para ejercer sus derechos, los usuarios pueden realizar una solicitud en https://www.el Prestador.com o por escrito mediante correo electrónico o carta postal a la dirección contacto especificada en el apartado **Datos de contacto de la organización**. En dicha petición, deberán adjuntar copia de su documento de identidad e indicar claramente cuál es el derecho que se desea ejercer.

9.5 Derechos de propiedad intelectual

9.5.1 Propiedad de la Declaración de Practicas de Certificación

Únicamente NOVOSIT goza de derechos de propiedad intelectual sobre esta Declaración de Prácticas de Certificación.

9.6 Obligaciones y responsabilidad civil

9.6.1 Obligaciones del Prestador

El Prestador garantiza, bajo su plena responsabilidad, que cumple con la totalidad de los requisitos establecidos en la DPCSCEC, siendo el responsable del cumplimiento de los procedimientos descritos, de acuerdo con las indicaciones contenidas en este documento.

El Prestador presta los servicios electrónicos de certificación conforme con esta DPCSCEC.

El Prestador informa al suscriptor de los términos y condiciones relativos a la prestación del servicio de comunicaciones electrónicas certificadas, de su precio y de sus limitaciones de uso, mediante un contrato de prestación de servicios.

El Prestador vincula a los suscriptores y terceros que confían en certificados, mediante esta DPCSCEC, en lenguaje escrito y comprensible, con los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en el presente documento.
- Límites de uso de los servicios de certificación.
- Forma en que se garantiza la responsabilidad patrimonial del Prestador de Servicios de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales el Prestador de Servicios de Certificación acepta o excluye su responsabilidad.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.

9.6.2 Obligaciones de terceros en el soporte de servicios al PSC

Las obligaciones de terceros en el soporte de los servicios que ofrece el PSC deben proporcionar, en líneas generales, las siguientes garantías:

- Cumplir y facilitar el cumplimiento de todo lo estipulado en esta DPCSCEC y en las políticas de certificación del PSC.
- Los servicios cuya infraestructura esté desplegada en terceros deben ofrecer los mismos niveles de seguridad y fiabilidad como si estuvieran desplegados en las infraestructuras del PSC.
- El tercero deberá conocer y seguir lo establecido en esta DPCSCEC y en las políticas de certificación, siendo de obligado cumplimiento como si del propio PSC se tratara.
- En el caso en el que el tercero, además, tenga que archivar información y datos, lo hará en las mismas condiciones y plazos que marcan la DPCSCEC y las políticas de certificación.
- El tercero deberá informar al PSC de cualquier cambio que se vaya a llevar en la infraestructura o en los procedimientos con el fin de someterlo a evaluación por parte del PSC. En cualquier caso, dichos cambios deberán garantizar lo estipulado en esta DPCSCEC y en las políticas de certificación.

9.6.3 Obligaciones de los suscriptores

Las obligaciones de los suscriptores con respecto a los servicios de certificación del Prestador son:

- Respetar lo dispuesto en esta DPCSCEC, así como en las prácticas y políticas del Prestador.
- Formalizar un contrato de prestación de servicios de certificación con el Prestador.
- Utilizar los servicios de certificación del Prestador de acuerdo con los procedimientos y, si es necesario, los componentes técnicos suministrados el Prestador, de conformidad con lo que se establece en la DPCSCEC y en la documentación del Prestador.
- Verificar las firmas electrónicas y los sellos de tiempos electrónicos, incluyendo la validez del certificado usado en los diferentes servicios de certificación del Prestador.
- Notificar cualquier incidente o hecho que afecte a los servicios de certificación del Prestador.

9.6.4 Garantías ofrecidas a suscriptores y terceros que confían

El Prestador, en la documentación que la vincula con suscriptores y terceros que confían, establece y rechaza garantías, y limitaciones de responsabilidad aplicables.

El Prestador garantiza al suscriptor que los servicios de certificación cumplen con todos los requisitos materiales establecidos en esta DPCSCEC, así como las normas de referencia.

El Prestador garantiza al tercero que confía en sus servicios de certificación que la información contenida o incorporada por sus servicios es correcta, excepto cuando se indique lo contrario.

9.6.5 Rechazo de otras garantías

El Prestador rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en el apartado 9.6.4 de este documento.

9.6.6 Limitación de responsabilidades

El Prestador limita su responsabilidad a la prestación de los servicios de certificación, los cuáles se regularán por el contrato oportuno.

El Prestador no será responsable de ningún daño directo y/o por terceros como consecuencia del uso indebido de los servicios de certificación.

9.6.7 Caso fortuito y fuerza mayor

El Prestador incluye en el contrato, cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

Se entiende por fuerza mayor todo acontecimiento extraordinario, imprevisible, irresistible y ajeno a la voluntad del Prestador, que imposibilite de forma temporal o definitiva el cumplimiento de las

obligaciones contractuales o regulatorias. Dentro de esta categoría se incluyen, a modo enunciativo más no limitativo, fenómenos naturales tales como huracanes, terremotos, inundaciones, incendios, así como hechos de autoridad, conflictos sociales, fallas generalizadas del suministro eléctrico u otros eventos de carácter externo que escapan al control del Prestador.

Por su parte, se considera caso fortuito aquel suceso imprevisto que, aunque derivado de la actividad o de los medios del propio Prestador, no pudo ser evitado pese a haberse adoptado todas las medidas de diligencia y previsión razonables.

En ambos casos, el Prestador quedará exento de responsabilidad por los perjuicios ocasionados al Usuario, siempre que acredite debidamente la ocurrencia del hecho.

9.6.8 Ley aplicable

NOVOSIT establece, en el contrato de suscriptor que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la Ley dominicana.

9.6.9 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

El Prestador establece, en el contrato de suscriptor, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.
- En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, la Entidad de Certificación vela porque, al menos los requisitos contenidos en las secciones **Obligaciones y responsabilidad**, **Auditoría de conformidad** y **Confidencialidad,** continúen vigentes tras la terminación del servicio y de las condiciones generales de emisión/uso.
- En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.

9.6.10 Cláusula de jurisdicción competente

El Prestador establece, en el contrato de, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces del país en el que el Prestador tiene autorización del Organismo Supervisor.

La competencia territorial y funcional se determinará en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

9.6.11 Resolución de conflictos

El Prestador establece, en el contrato de suscriptor, los procedimientos de mediación y resolución de conflictos aplicables.

10Anexo I - Acrónimos

A continuación, se muestran los acrónimos utilizados en la presente DPCSCEC.

- AC: Autoridad de Certificación. También se puede utilizar CA (*Certification Authority*).
- CPD: Centro de Procesamiento de Datos.
- DPC: Declaración de Prácticas de Certificación. También se puede utilizar CPS (*Certification Practice Statement*).
- DPCSCEC : Declaración de Prácticas de Certificación del Servicio de Comunicaciones Electrónicas Certificadas.
- ETSI: *European Telecommunications Standards Institute* o Instituto Europeo de Normas de Telecomunicaciones.
- ISO: International Organization for Standardization. Organismo Internacional de Estandarización.
- NTP: *Network Time Protocol*.
- OCSP: *On-line Certificate Status Protocol*. Protocolo de acceso al estado de los certificados.
- OTP: *One-Time Password*.
- PSC: Prestador de Servicios Electrónicos de Certificación / Confianza.