BANCO CENTRAL DE COSTA RICA

DIVISIÓN SISTEMAS DE PAGO

ESTÁNDAR SOPORTE

FIRMA DIGITAL

SERIE DE NORMAS Y PROCEDIMIENTOS

Público

sinpe

ES-FDI

BANCO CENTRAL DE COSTA RICA

DIVISIÓN SISTEMAS DE PAGO

E S T Á N D A R S O P O R T E

F I R M A D I G I T A L

SERIE DE NORMAS Y PROCEDIMIENTOS

Público

sinpe

ES-FDI

Tabla de contenido

1. Introducción **1**
2. Alcance **2**
3. Términos empleados **2**
4. Documentos aplicables y anexos **3**
5. Especificaciones técnicas **3**
5.1. Centro de Soporte 3
5.2. Plataformas tecnológicas 5
5.3. Call Center (Centro de Llamadas) 6
5.4. Acceso Remoto 7
5.5. Sitio Web 8
5.6. Instaladores 9
5.7. Escalamiento de casos 10
5.8. Personal de soporte 11

Sistema Nacional de Pagos Electrónicos

1. Introducción

En el 2005 se aprobó la ley de firma digital en Costa Rica. Esta ley permite llevar al mundo electrónico la relevancia jurídica de la firma autógrafa, otorgando igual funcionalidad entre ambos tipos de firma. La firma digital se puede realizar cuando una persona posee un dispositivo de seguridad personalizado de forma exclusiva y que contiene sus certificados digitales. Los certificados digitales son documentos electrónicos que contienen información de la persona y que sirven para validar su identidad. En Costa Rica, obligatoriamente, los certificados digitales tienen que ser emitidos por una autoridad certificadora (CA por sus siglas en inglés) registrada ante el Ministerio de Ciencia y Tecnología (MICIT) y en dispositivos de seguridad que satisfacen los requerimientos especificados en la ley.

El BCCR, en coordinación con el Sistema Financiero Nacional (SFN) implementó una autoridad certificadora llamada CA SINPE - PERSONA FISICA, la cual está debidamente registrada ante el MICIT. En adelante, dicha CA se denominará CA SINPE.

Por medio de la plataforma del Sistema Nacional de Pagos Electrónicos (SINPE), se ofrece el servicio de Firma Digital, con la meta de emitirle, a un bajo costo, certificados digitales a los ciudadanos costarricenses y a los extranjeros residentes en el país. Las entidades asociadas al SINPE que participan del servicio de Firma Digital se conocen como Oficinas de Registro (OR). En las OR se realiza el trámite de registro y entrega de los dispositivos de seguridad y los certificados correspondientes; las cuales están ubicadas a lo ancho de todo el país. No todas las entidades asociadas al SINPE ofrecen el servicio de Firma Digital, pues participar de dicho servicio es opcional para las entidades asociadas al SINPE.

El MICIT definió como parte de sus políticas los requerimientos básicos de los dispositivos de seguridad que las autoridades certificadoras tienen que usar para emitir certificados digitales. Con base en estos requisitos CA SINPE decidió utilizar tarjetas inteligentes como los dispositivos de seguridad en los cuales emitir los certificados digitales.

Estos dispositivos criptográficos también tienen que cumplir una serie de requerimientos adicionales a los definidos por el MICIT que garantizan su funcionamiento adecuado en el servicio de Firma Digital de la CA SINPE. Por esta razón, CA SINPE realiza periódicamente procesos de homologación cuyo resultado es una lista de marcas y modelos de los dispositivos criptográficos que las OR pueden comprar de acuerdo a sus intereses institucionales.

Los ciudadanos o residentes que se suscriben a CA SINPE, son llamados suscriptores. Ellos reciben en un dispositivo criptográfico (tarjeta inteligente) dos certificados digitales, uno que sirve para autenticación y otro para firma digital. Si los certificados se entregan en tarjeta inteligente, y el suscriptor lo desea, recibe también el lector de tarjetas inteligentes.

Los certificados tienen una vigencia de dos años, por lo que cada vez que a un suscriptor se le venzan los certificados, y si éste desea renovarlos, deberá acudir de nuevo a una OR para que le emitan los nuevos certificados. La renovación de los certificados se puede hacer en el mismo dispositivo criptográfico, siempre y cuando esté se encuentre en buen estado.

Como parte del marco normativo que rige la operación del servicio de Firma Digital, se ha establecido que cuando una OR entrega al suscriptor un dispositivo criptográfico con los certificados correspondientes, la OR está en la obligación de brindar al cliente un servicio de soporte técnico, ya sea propio o contratado, que le garantice a sus clientes, tener la ayuda de personal calificado en la instalación de todo el software que controla los dispositivos y en la configuración de su equipo de cómputo para que opere adecuadamente con los certificados de CA SINPE.

En complemento de dicho marco normativo, la CA SINPE ha decidido también normar las características del servicio con el propósito de estandarizar el servicio de soporte y lograr con ello mayor eficiencia y asegurar su calidad hacia el cliente final, los suscriptores.

Este documento describe todas las características que deben estar presentes en el servicio de soporte que las OR brinden a los suscriptores de firma digital de la CA SINPE, de forma que se pueda garantizar a todos sus suscriptores, independientemente de la OR en donde reciban su certificado, un servicio de soporte técnico de alta calidad en la instalación de los dispositivos criptográficos, configuración del equipo de cómputo y uso de los certificados digitales durante toda la vigencia de los mismos.

2. Alcance

Este estándar aplica a todas las entidades asociadas al SINPE que se hayan suscrito al servicio de Firma Digital.

3. Términos empleados

Para los fines del presente documento, se entenderá por:

- Acuerdo suscriptor:
- BCCR: Banco Central de Costa Rica.
- CA SINPE: Autoridad Certificadora del Sistema Nacional de Pagos
- MICIT: Ministerio de Ciencia y Tecnología,.
- SINPE: Sistema Nacional de Pagos Electrónicos.

Para consultar algún otro término que aparezca en este documento, remítase a la “Norma complementaria - Glosario general”.

4. Documentos aplicables y anexos

Siglas	Nombre del documento
Ley 8454	Ley de Certificados, Firmas Digitales y Documentos Electrónicos
Reglamento - Ley 8454	Reglamento a La Ley de Certificados, Firmas Digitales y Documentos Electrónicos
RSP	Reglamento del Sistema de Pagos
OID 2.16.188.1.1.1.1 Versión: 1.00	Política de Certificados para la Jerarquía Nacional de Certificadores Registrados
OID 2.16.188.1.1.1.1 Versión: 1.00	Directrices para las Autoridades de Registro. Características de Cumplimiento de Autoridades de Registro (RA) de la Jerarquía Nacional de Certificadores Registrados de Costa Rica
NC - GGE	Norma complementaria - Glosario general.
NC - FID	Norma Complementaria – Firma Digital
EE - FID	Estándar Electrónico – Firma Digital
EF- FID	Estándar Físico – Firma Digital

5. Especificaciones técnicas

5.1. Centro de Soporte

El servicio de soporte debe brindarse por medio de un Centro de Soporte formalmente establecido que posea la infraestructura tecnológica necesaria para proveer el servicio con las características que se especifican en este estándar.

El Centro de Soporte debe ofrecer un horario corrido de lunes a viernes de 8:00 a.m. a 6:00 p.m. y sábados de 8:00 a.m. a 5:00 p.m. El servicio de soporte técnico debe brindarse en idioma español e inglés. El servicio en inglés puede brindarse en un horario menor, al establecido anteriormente, siempre y cuando se garantice la atención en este idioma inglés todos los días (de lunes a sábado).

El Centro de Soporte debe atender a todas las personas que tengan certificados digitales activos emitidos por CA SINPE. Debe brindarse soporte técnico al suscriptor todas las veces que lo requiera y en cualquier equipo de cómputo que éste indique. Si el suscriptor requiere realizar múltiples instalaciones en diferentes equipos se deberán atender todas las instalaciones o configuraciones que sean necesarias. Además, debe atenderse al suscriptor cuando requiera ayuda por primera vez o en casos reincidentes, independientemente de la razón que los haya ocasionado, por ejemplo: virus, corrupción de archivos, bloqueo de puertos, instalaciones de hardware o software conflictivo, etc.

Un certificado digital se considera activo a partir de que el suscriptor firma el Acuerdo de Suscriptor y por el período de vigencia del certificado, excepto que el suscriptor lo revoque antes de su vencimiento.

CA SINPE implementará un mecanismo para que el Centro de Soporte, que la OR designe, se entere de la activación de cada uno de los certificados digitales. La finalidad de este mecanismo es que tanto la OR como la CA SINPE controlen los certificados que son objeto de soporte técnico.

La OR debe entregarle al suscriptor junto con el certificado digital la información del Centro de Soporte Técnico que le atenderá cuando requiera ayuda. La OR debe entregar esta información impresa al reverso de la tarjeta inteligente siguiendo lo especificado en el Estándar Físico Firma Digital en el Anexo 8. De forma transitoria la OR podrá entregar la información de forma impresa en cualquier otro medio, siempre y cuando como mínimo se consigne al menos los siguientes datos: número de teléfono, dirección de correo electrónico y dirección del sitio web del Centro de Soporte.

Cuando el suscriptor solicite el servicio de soporte, éste deberá facilitarse por teléfono, chat o correo electrónico, según el gusto del suscriptor. Asimismo, ya sea por complejidad técnica del caso o por preferencia del suscriptor, el servicio también deberá proporcionarse por medio de acceso remoto al computador correspondiente. Para hacer acceso remoto al computador del suscriptor se debe contar previamente con el visto bueno del suscriptor las veces que sea necesario brindar este tipo de soporte. En la medida de lo posible deberá recurrirse a ellas hasta haber agotado todas las posibilidades por vía telefónica, chat o correo electrónico.

Para la atención vía chat, la herramienta que utilice el Centro de Soporte, no debe imponer restricciones adicionales a los usuarios finales por ejemplo, abrir puertos especiales en el Firewall, instalar software cliente, o limitarse a sistemas operativos particulares.

El nivel de servicio debe ser como mínimo del 90% en 30 segundos, es decir que el 90% de las llamadas deben ser atendidas en menos de 30 segundos. Por otro lado, el nivel de servicio para las solicitudes recibidas por correo electrónico o chat deberá ser del 100% en 2 horas hábiles, es decir atender el 100% de los correos electrónicos recibidos en no más de 2 horas hábiles siguientes a la recepción del correo.

El Centro de Soporte debe tener un procedimiento que describa detalladamente los pasos, roles y registros que se siguen en la atención de casos. Este procedimiento debe considerar, como mínimo, el registro de los datos de contacto del suscriptor, la verificación del dispositivo criptográfico, la información que el soportista le brinda al suscriptor, los pasos que se siguen de acuerdo a la modalidad de atención (teléfono, chat o acceso remoto), las pruebas que se aplican dependiendo del tipo de caso, los mecanismos de escalamiento y resolución, el tratamiento que se le da a los casos pendientes de resolver, el cierre de casos ya resueltos, etc.

El Centro de Soporte debe contar con un mecanismo para garantizar que todas las llamadas telefónicas, chats, correos electrónicos y sesiones remotas que se realicen como parte de la prestación del servicio de soporte quedan grabadas en su totalidad sin que medie acción alguna por parte del agente de soporte. Además el Centro de Soporte debe contar con un esquema de respaldos que asegure que los archivos correspondientes a las grabaciones se mantendrán almacenados e íntegros al menos por 1 año para la verificación posterior.

El Centro de Soporte debe contar con un sistema de información automatizado, que permita el registro y seguimiento de los casos atendidos. El sistema deberá registrar si fue requerido acceso remoto para efectos generar estadísticas.

Además, en este sistema se deberá documentar la información de contacto tal como:

- Cédula del contacto
- Nombre completo
- Sistema Operativo del usuario final: Service Pack y si se trata de una plataforma de 32 o 64 bits
- Descripción del problema
- Diagnóstico Inicial
- Solución brindada.
- Estado del caso .
- Fecha de Apertura.
- Oficina de Registro en donde se gestionó el certificado digital.

El Área de Vigilancia del SINPE podrá solicitar en cualquier momento acceso a los reportes, bitácoras o mecanismos de monitoreo que se definan en este estándar, con el fin de supervisar el cumplimiento de este estándar y la calidad del servicio de soporte técnico ofrecido por la OR.

5.2. Plataformas tecnológicas

Por política y de acuerdo con lo estipulado en la Ley 8454, el Banco Central de Costa Rica (BCCR) debe respetar el principio de neutralidad para las tecnologías involucradas. Por esta razón, el servicio de soporte técnico debe brindarse como mínimo, para plataformas de 32 y de 64 bits y para los siguientes sistemas operativos:

- Microsoft Windows Mac OS-X
- Linux, al menos la distribución de Ubuntu.

  Además, deberá brindarse soporte técnico a los navegadores propietarios a cada uno de los sistemas operativos indicados: Internet Explorer y Safari. Y también al navegador de uso libre Mozilla Firefox, que soporta certificados digitales y que trabaja en cualquiera de los sistemas operativos indicados. El servicio de soporte técnico también deberá brindarse para las siguientes aplicaciones de escritorio Office, Open Office y Adobe, independientemente del sistema operativo bajo el cual corran. Así como, a las herramientas de correo electrónico Microsoft Outlook para los sistemas operativos en donde corre y Thunderbird para las versiones de Linux a las que se les da soporte.

A continuación se presenta un cuadro que resume la infraestructura tecnológica que es parte del alcance del servicio de soporte técnico que se debe brindar al suscriptor. Además, el cuadro indica claramente el driver sobre el cual los dispositivos criptográficos funcionan con las herramientas antes indicadas.

De esta forma el Centro de Soporte, como parte del servicio que ofrece, podrá guiar al suscriptor cuando esté utilizando una aplicación que use certificados digitales de la Jerarquía Nacional y que ha sido desarrollada a lo interno de cualquier organización.

	Windows		Macintosh		Linux
	XP SP3 o superior		MAC OS-X 10.5 o superior		Ubuntu 11+
Driver	Mini driver	PKCS#11	Tokend	PKCS#11	PKCS#11
Navegador	I.E. 7+	Firefox 3.6+	Safari 5+	Firefox 3.6+	Firefox 3.6+
Aplicación de escritorio	MS Office 2007+	Open Office Adobe Reader X Pro	-	Open Office Adobe Reader X Pro	Open Office Adobe Reader X Pro
Correo electrónico	MS Outlook 2007+	Thunderbird 3.1.7+	MS Outlook para Mac 2011+	Thunderbird 3.1.7+	Thunderbird 3.1.7+

Finalmente, como parte de la política del soporte técnico al usuario final, cuando una versión de los sistemas operativos o herramientas antes indicados deja de ser soportada por el fabricante automáticamente podrá dejar de ser soportada por el Centro de Soporte Técnico al usuario final. Las versiones que el fabricante libere en modalidad Beta, no será obligatorio que el Centro de Soporte les brinde soporte; sin embargo, es recomendable que el Centro de Soporte prepare su servicio alrededor de ellas pues toda nueva versión que el fabricante libere en producción deberá automáticamente empezar a ser soportada por éste.

5.3. Call Center (Centro de Llamadas)

Para la atención telefónica, el Centro de Soporte debe proporcionar un único número telefónico y poseer un sistema tipo “Call Center” automatizado que sea quien administre ese número de teléfono y que permita la recepción de llamadas y el enrutamiento inteligente de las mismas.

Como mínimo la plataforma de “Call Center” deberá contar con la capacidad de recibir hasta 30 llamadas de forma simultánea y una vez que una llamada ingrese se deberá escuchar un Mensaje de Bienvenida y el sistema deberá trasladarla al agente disponible con el perfil más adecuado para atenderla. En caso de que todos los agentes se encuentren ocupados, el sistema deberá anunciar mensajes de espera y pasar la llamada a la cola de espera; durante el tiempo que el suscriptor esté esperando se deberá escuchar algún sonido o mensaje que le indique a la persona que aún su llamada se encuentra activa.

En caso de que la espera supere los 30 segundos, el sistema de “Call Center” deberá implementar el servicio de devolución de llamada, para lo cual el sistema deberá informarle al usuario final la transferencia de su llamada a un sistema interactivo de voz (IVR). El IVR deberá solicitar como mínimo el nombre, número de teléfono del usuario y horario preferido para la devolución de la llamada.

El Centro de Soporte debe contar con procedimientos para garantizar que en todos los casos que el usuario final haya dejado sus datos en el sistema IVR, se le devolverá la llamada para atender su requerimiento.

La plataforma de “Call Center” debe contar con la capacidad de habilitar números adicionales a los cuales se les pueda dar tratamientos diferenciados, de forma tal que por DNIS (número marcado) se pueda realizar el enrutamiento y tratamiento especial de las llamadas.

La plataforma de “Call Center” debe registrar y monitorear en tiempo real, el estado de los agentes de soporte. Al menos se deben registrar y monitorear los estados: Login, Logout, No Listo.

La plataforma de “Call Center” debe registrar y monitorear en tiempo real la actividad de las colas de atención de llamadas y de espera, de forma tal que se pueda registrar y monitorear, al menos la siguiente información:

- Total de Llamadas Entrantes,
- Total de Llamadas Contestadas,
- Total de Llamadas Abandonadas,
- Tiempo Promedio de Conversación,
- Nivel de Servicio Ofrecido.

La plataforma de “Call Center” debe permitir el monitoreo silencioso de las llamadas y en caso de ser necesario la intervención de las mismas, por parte del Coordinador del Centro de Soporte o de cualquier persona que la OR o la CA SINPE asignen.

De forma automática, la plataforma de “Call Center” debe proveer reportes históricos en los cuales conste al menos la siguiente información, niveles de servicio, total de llamadas entrantes, total de llamadas atendidas, tiempos promedios de espera, tiempos promedios de conversación y niveles de abandono.

5.4. Acceso Remoto

Para brindar el soporte remotamente, el Centro de Soporte deberá contar con licencias de software para el uso de una herramienta que le permita hacer acceso remoto a los computadores de los suscriptores en forma segura.

Dado que el acceso remoto a las computadoras del suscriptor solo debe ser realizado con el previo consentimiento del suscriptor, esta herramienta debe contar con un mecanismo para que antes de ingresar al equipo, el suscriptor deba obligatoriamente aprobar el acceso mediante una acción, por ejemplo un clic en el botón aceptar asociado a un mensaje de advertencia. El mensaje debe encontrarse en español y en inglés.

La herramienta de acceso remoto deberá tener las siguientes características:

- Debe ser una herramienta web de forma que no se requiera instalar nada en el computador del usuario.
- Control automatizado para que no se pueda hacer acceso remoto al computador del usuario sin que éste lo haya autorizado explícitamente en el sistema.
- Mecanismos de control de acceso que debe dejar registrado el usuario que efectuó el acceso al computador del usuario final.
- Bitácoras que registren todos los eventos sucedidos durante la sesión remota.

- ⊡ Mecanismo que le permita al usuario tener siempre el control de su computador y visualizar completamente lo que sucede durante la sesión remota. Además, el usuario final tendrá que estar habilitado en todo momento para terminar la sesión remota en el momento que lo desee, sin que tenga que intervenir para ello el soportista.
- ⊡ Cifrado de la comunicación extremo a extremo (del equipo del soportista al equipo del usuario final). El cifrado debe ser al menos de 128 bits, bajo el algoritmo AES.
- ⊡ Permitir establecer una sesión de chat, donde el agente de soporte y el suscriptor puedan comunicarse durante toda la sesión remota.
- ⊡ Permitir el envío y recepción de archivos, con los controles suficientes para garantizar que el suscriptor siempre tiene la forma de aceptar o rechazar la recepción de un archivo.
- ⊡ Permitir reiniciar el equipo y reconectarse a la sesión remota de forma automática, es decir, que cuando el proceso de soporte requiera que el equipo sea reiniciado, la herramienta de acceso remoto permita restaurar la sesión remota sin necesidad de establecerla como si fuera una nueva sesión, luego de que el suscriptor ingrese a su equipo.
- ⊡ Proveer reportes que permitan controlar las sesiones realizadas, revisar grabaciones y conversaciones en chat.
- ⊡ Grabación de la sesión remota de forma completa (de principio a fin) y sin que medie acción alguna por parte del soportista. Estas grabaciones deben incluir la conversación de chat, la grabación de pantallas, así como todas las acciones acontecidas durante la sesión remota. La grabación debe iniciar automáticamente apenas se establece la sesión remota.
- ⊡ Tener la capacidad para almacenar las grabaciones por al menos 1 año.
- ⊡ Todo registro almacenado (bitácoras, grabaciones, etc.) debe ser trazable para que se sepa quién fue el soportista que atendió el caso y cuándo fue atendido.

5.5. Sitio Web

Como parte del servicio de soporte se tiene que proveer un sitio Web expuesto en Internet y exclusivo para los temas de soporte técnico de Firma Digital que brinda la OR. El dominio correspondiente al sitio Web debe ser propiedad de la OR o de la empresa a quien la OR le contrató el servicio. El Sitio Web debe tener un porcentaje de tiempo disponible de al menos 99%.

El Sitio Web debe mostrar todo su contenido en idioma Español e Inglés y debe contener la información suficiente para que una persona pueda aclarar por su propia cuenta las dudas que tenga respecto al uso de los certificados digitales y de la firma digital.

El sitio Web debe exponerse como sitio seguro; es decir debe tener un certificado SSL válido y emitido por una autoridad certificadora reconocida.

El certificado SSL debe ser de al menos 128 bits, estar vigente y debe haber sido emitido por una Autoridad Certificadora de Confianza, reconocida por los fabricantes de los sistemas operativos y de los navegadores indicados en la sección 5.2, de forma que su cadena de certificación quede instalada automáticamente con la instalación del sistema operativo y navegador tal y como vienen de fábrica.

El contenido mínimo del Sitio Web deberá ser:

1. Número de teléfono del Centro de Soporte y horario de atención.
2. Sección de preguntas y respuestas, la cual deberá ser actualizada, al menos una vez al mes, con las lecciones aprendidas por los problemas y soluciones de los casos de soporte atendidos.
3. Una sección de información general acerca de los certificados digitales y su funcionalidad.

4. Información actualizada de los sistemas operativos y los navegadores en que son soportados los dispositivos criptográficos homologados por CA SINPE.
5. Un link al URL definido para la revocación de certificados, desde el cual una persona pueda proceder con la revocación de los certificados digitales en caso de que lo requiera.
6. Un link desde el cual se pueda abrir una sesión de chat para hacer contacto con el personal del Centro de Soporte.
7. Un link para que el suscriptor pueda enviar un correo electrónico al Centro de Soporte.
8. Un link que le facilite al suscriptor el acceso a la herramienta que le permitirá al Centro de Soporte acceder remotamente la computadora del suscriptor.
9. Funcionalidad de autenticación y firma digital de forma que el suscriptor pueda corroborar la operación correcta de su dispositivo criptográfico y los certificados digitales emitidos por CA SINPE. Como parte de la funcionalidad de autenticación y firma digital se debe implementar la verificación en tiempo real de la validez de los certificados digitales emitidos por CA SINPE, para lo cual, como mínimo se debe considerar:
   - **a)** Pertenencia de los certificados a la Jerarquía Nacional de Certificación Digital, en concordancia con la Política de Certificados para la Jerarquía Nacional de Certificadores Registrados.
   - **b)** Período de vigencia del certificado de forma que se verifique que no estén vencidos o que no sean vigentes solo en el futuro.
   - **c)** Que el OID de los certificados para autenticarse al sitio sea el 2.16.188.1.1.1.1.3 y que los certificados usados para probar la funcionalidad de firma digital tengan el OID 2.16.188.1.1.1.1.2.
   - **d)** Que en el dispositivo criptográfico se encuentre almacenado un certificado digital para autenticación y otro para firma digital.
   - **e)** Que los certificados no estén revocados. La verificación de revocación debe implementarse utilizando los servicios de validación en tiempo real (OCSP) publicados por CA SINPE.
   - **f)** Firmar un documento digitalmente en el lado del cliente con el certificado de firma digital.
   - **g)** Verificar en el lado del servidor la firma digital del documento recién firmado.
10. Opción para que los suscriptores puedan descargar o ejecutar desde el mismo sitio, los programas instaladores, detallados en el punto 5.6.
11. Las guías que el Centro de Soporte desarrolle como parte del servicio de soporte de firma digital, disponibles para su descarga por el suscriptor, las cuales al menos deben contemplar: guías para que el suscriptor pueda verificar la vigencia de su certificado, cambiar el pin ante una OR o bien desde su propio computador, emisión de un nuevo certificado usando el mismo dispositivo, pasos para firmar un documento y cualquier otra necesaria que contribuya al buen uso de los certificados y la mejora del servicio de soporte.

5.6. Instaladores

Los instaladores son programas cuya funcionalidad debe permitir ejecutar paso a paso y de forma desatendida la instalación de los drivers de todos los modelos de dispositivos criptográficos que la OR entregue y que previamente han sido homologados por CA SINPE.

Los instaladores deben configurar en forma automática la computadora del suscriptor, de forma que ésta quede completamente lista para el adecuado funcionamiento de los certificados digitales contenidos en los dispositivos criptográficos.

Los instaladores deben correr en los mismos ambientes en que opera el servicio de soporte, los cuales fueron descritos en el punto 5.2.

Los instaladores deben desplegar mensajes que informen al suscriptor durante todo el proceso de instalación los pasos que se están realizando, además deben guiar al suscriptor para que una vez finalizada la ejecución de los programas instaladores, el suscriptor realice la verificación de los certificados digitales, mediante la navegación automática al Sitio Web del Centro de Soporte, a la opción de autenticación con certificado digital y firma digital de un documento electrónico, detallado en el punto 5.5.

Los instaladores deben ejecutar las acciones necesarias para que todas las herramientas o aplicaciones indicadas en la sección 5.2 que corren en las computadoras del suscriptor queden configuradas adecuadamente para el funcionamiento de los certificados digitales de CA SINPE. Por ejemplo, y sin limitarse a esto, incluir los Sitios Web en los sitios de confianza del IE, instalar componentes requeridos para que el sitio funcione adecuadamente, tales como Microsoft Capicom, Java, etc.

Los instaladores deben configurar las herramientas cliente que estén instaladas en la computadora para que queden listas para firmar digitalmente o para reconocer documentos firmados digitalmente y validar las firmas. Por ejemplo, Microsoft Office, Microsoft Outlook, Adobe, etc.

Los programas instaladores deben instalar en los contenedores requeridos por las aplicaciones que se encuentran en el computador del suscriptor los certificados digitales correspondientes a la Jerarquía Nacional de Certificación Digital, a saber los certificados CA RAIZ NACIONAL – COSTA RICA, CA POLITICA PERSONA FISICA – COSTA RICA, CA SINPE – PERSONA FISICA.

Los casos que el Centro de Soporte considere necesario atender por medio de guías, por ejemplo la instalación o configuración de algunos componentes que el instalador no pueda ejecutar en forma desatendida, deberán ser justificados a la CA SINPE y ésta se reserva el derecho de no aceptar la solución y pedir a la OR o cuando aplique al Centro de Soporte que se programen las rutinas correspondientes para automatizar la solución.

Los programas instaladores se deberán actualizar periódicamente, cada vez que existan nuevas versiones de los drivers de los dispositivos criptográficos, la CA SINPE homologue nuevos dispositivos o según los requerimientos de actualización que se presenten en los sistemas operativos soportados y plataformas soportadas.

5.7. Escalamiento de casos

El servicio de soporte técnico debe diferenciar las solicitudes que se generan por problemas de los dispositivos criptográficos o certificados digitales, de las solicitudes que se generan por problemas con los sistemas o aplicaciones desarrollados por las organizaciones o instituciones del país y que hacen uso de los certificados digitales.

Como parte del servicio se deberán aceptar todas las solicitudes y hacer las pruebas básicas para determinar si el problema es en los dispositivos criptográficos o certificados digitales o, en la aplicación o sistemas que hacen uso de los mismos. Cuando se corrobore que el problema no está relacionado con los dispositivos criptográficos o los certificados digitales propiamente, sino con el sistema o aplicación que hace uso de los mismos, el Centro de Soporte deberá trasladar el caso a la organización dueña de la aplicación con problemas.

Como parte de los procedimientos de atención de casos el Centro de Soporte debe contemplar la atención de los casos que se generan por problemas en los sistemas o aplicaciones que hacen uso de los certificados digitales y no por problemas en los dispositivos criptográficos o en los certificados en sí. Este procedimiento debe tener documentada la forma en cómo se traslada un caso de soporte con la organización dueña de la aplicación o sistema que presenta el problema y los parámetros que indican que el suscriptor quedó satisfecho con la atención recibida e informado de la realidad de la situación.

Para todos los casos en donde el problema debe ser atendido por el Centro de Soporte, éste debe implementar un esquema de escalamiento de forma que el caso se atienda de la siguiente forma:

- Primer Nivel: Un Agente de Soporte debe ser el primer punto de contacto entre el suscriptor y el Centro de Soporte.
- Segundo Nivel: Después de un plazo máximo de 2 horas hábiles sin haber resuelto el caso, el Agente de Soporte debe escalar el caso a un Ingeniero de Soporte.
- Tercer Nivel: Después de un plazo máximo de 8 horas hábiles sin haber resuelto el caso, el Ingeniero de Soporte debe escalar el caso al fabricante correspondiente. Al respecto, se debe considerar que el fabricante puede ser: el desarrollador de los drivers y del middleware de los dispositivos criptográficos, el fabricante propiamente del hardware de los dispositivos criptográficos, el desarrollador de los sistemas operativos sobre los cuales se están instalando los dispositivos criptográficos o el desarrollador de cualquier otro software que esté afectando el funcionamiento correcto de los dispositivos o los certificados digitales.

Para garantizar el tercer nivel de soporte, el Centro de Soporte, ya sea propio de la OR o contratado por ésta; debe contar con una certificación que haga constar que cuenta con el respaldo de los fabricantes involucrados, de acuerdo a lo señalado en el párrafo anterior.

5.8. Personal de soporte

El personal del Centro de Soporte debe ser suficiente en cantidad y calidad para dar el servicio de soporte a todos los suscriptores de CA SINPE que hayan solicitado su certificado en la OR, atendiendo el nivel de servicio especificado en la sección 5.1. Dentro de los roles del Centro de Soporte se deben tener Agentes de Soporte, Ingenieros de Soporte y Coordinador del Centro de Soporte.

Las funciones de los Agentes de Soporte deberán ser:

- atender de primera entrada al suscriptor; es decir, ser el primer punto de contacto entre el usuario final y el Centro de Soporte.
- guiar y ayudar al suscriptor a solventar cualquier problema que tenga con los dispositivos criptográficos o con los certificados digitales emitidos por CA SINPE.
- escalar al Ingeniero de Soporte los casos que no haya podido resolver y que ya hayan alcanzado el límite de tiempo establecido para el soporte de primer nivel.
- mantener comunicación periódica con el suscriptor respecto al estado del caso mientras éste se encuentre escalado a segundo o tercer nivel.
- cualquier otra función que la CA SINPE advierta a las OR con el fin de mejorar la calidad del servicio de soporte técnico a sus suscriptores.

Las funciones de los Ingenieros de Soporte deberán ser:

- ⊡ brindar el soporte a segundo nivel.
- ⊡ desarrollar y mantener actualizados los programas instaladores para todas las plataformas y sistemas operativos indicados anteriormente.
- ⊡ desarrollar y mantener actualizado el Sitio Web de Soporte de Firma Digital.
- ⊡ cuando la CA SINPE esté ejecutando procesos de homologación o cualquier prueba aislada de dispositivos criptográficos, ejecutar las pruebas de compatibilidad de los drivers en los sistemas operativos indicados por CA SINPE.
- ⊡ investigar las causas de un problema y buscar las posibles soluciones a cualquier problema que se esté presentando con los dispositivos criptográficos y con los certificados emitidos por CA SINPE.
- ⊡ escalar a los fabricantes correspondientes todos los casos que no haya podido resolver y que ya hayan alcanzado el límite de tiempo establecido para el soporte de segundo nivel.
- ⊡ mantener la comunicación periódica con el Agente de Soporte respecto al estado del caso mientras éste se encuentre escalado a segundo o tercer nivel.
- ⊡ cualquier otra función que la CA SINPE advierta a las OR con el fin de mejorar la calidad del servicio de soporte técnico a sus suscriptores.

Las funciones del Coordinador del Centro de Soporte deberán ser:

- ⊡ atender todos los requerimientos que la CA SINPE establezca respecto al servicio de soporte técnico.
- ⊡ garantizar la calidad de servicio que se está brindando a los suscriptores.
- ⊡ responder a todos los requerimientos que la CA SINPE tenga como parte de sus funciones de supervisión y vigilancia.
- ⊡ cualquier otra función que la CA SINPE advierta a las OR con el fin de mejorar la calidad del servicio de soporte técnico a sus suscriptores.

El personal del Centro de Soporte debe cumplir al menos con los siguientes requisitos:

- ⊡ Conocimientos técnicos avanzados en soporte para las plataformas Microsoft Windows XP, Vista y Windows 7.
- ⊡ Conocimientos comprobables en distribuciones Linux y Macintosh.
- ⊡ Conocimientos comprobables en las herramientas o aplicaciones indicadas en la sección 5.2.
- ⊡ Experiencia en las herramientas para desarrollo de aplicaciones web.
- ⊡ Experiencia en servicios de atención al cliente y en soporte técnico.

El personal del Centro de Soporte se debe mantener actualizado en las tecnologías de usuario final (sistemas operativos, ambientes web, navegadores, actualizaciones, etc.), en las características y funcionalidades de las diferentes versiones de software, middleware y firmware de los dispositivos homologados por CA SINPE y en servicio al cliente.

La OR está en la obligación de garantizar que el personal que brinda el servicio de soporte, ya sea propio de la OR o por medio del contrato establecido con alguna empresa de soporte reciba capacitación recibida directa de los fabricantes del hardware y software de los dispositivos criptográficos que la OR entrega a los suscriptores.

El Centro de Soporte debe contar con un área de Investigación y Desarrollo que se encargue de la investigación de casos de solución compleja, así como el desarrollo de instaladores y continuo mejoramiento del sitio web solicitado en los requerimientos. Los puestos dentro de esta área deben ser ocupados por Ingenieros de Soporte de acuerdo al perfil descrito anteriormente.

El personal del Centro de Soporte debe poseer una certificación otorgada por el fabricante del hardware y del middleware de los dispositivos criptográficos homologados y también por el fabricante de los sistemas operativos soportados.