



MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Página 1
	Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay	Anexo de la Resolución N° <u>1399-</u>

CARACTERÍSTICAS MÍNIMAS DE SEGURIDAD PARA LA AUTORIDADES DE REGISTRO DE LA INFRAESTRUCTURA DE CLAVES PÚBLICAS DEL PARAGUAY

DOC-PKI-05 Versión 1.0


Abog. Rodolfo Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico



MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Pagina 2
	Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay	Anexo de la Resolución N° _____

CONTROL DOCUMENTAL


Documento	
Título: Características Mínimas de Seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay.	Nombre Archivo:
Código: DOC-PKI-05	Soporte Lógico:
Fecha: 28/10/2016	Ubicación Física: DGFDyCE
Versión: 1.0	


Registro de Cambios		
Versión	Fecha	Motivo de Cambio

Distribución del Documento	
Nombre	Área
Ministerio de Industria y Comercio (MIC)	Dirección General de Firma Digital y Comercio Electrónico (DGFDyCE)
Autoridad Certificadora (CA)	Prestadores de Servicio de Certificación (PSC)
Documento Público	www.acraiz.gov.py

Control de Documento		
Preparado por:	Revisado por:	Aceptado por:
Ing. Lucas Sotomayor	Lic. Noelia Smith	M. Sc. Rodys Rolón

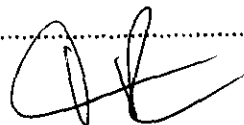

 Abog. Rodys Rolón A.
 DIRECTOR GENERAL
 Firma Digital y Comercio Electrónico




<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 3</p>
	<p>Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay</p>	<p>Anexo de la Resolución N° <u>1399-</u></p>

Contenido

1. DISPOSICIONES GENERALES	4
2. SEGURIDAD PERSONAL.....	8
2.1. DISPOSICIONES GENERALES.....	8
2.2. DOCUMENTACIÓN DEL AGENTE DE REGISTRO	8
2.3 ENTRENAMIENTO DEL AGENTE DE REGISTRO	10
2.4. ACOMPAÑAMIENTO PERIÓDICO.....	11
2.5. SUSPENSIÓN Y TERMINACIÓN.....	11
3. SEGURIDAD FÍSICA	12
3.1 LAS INSTALACIONES TÉCNICAS Y LOS PUESTOS TEMPORALES DE UNA RA PUEDEN SER DE 2 TIPOS:.....	12
3.2 EN AMBOS CASOS, SE APLICAN LOS SIGUIENTES REQUISITOS MÍNIMOS DE SEGURIDAD:.....	12
3.3 PARA LAS RA QUE TENGAN UN ENTORNO DEDICADO, APLICARÁ, ADEMÁS DE LAS EXIGENCIAS DEL ÍTEM 3.2, TAMBIÉN LOS SIGUIENTES REQUISITOS DE SEGURIDAD:.....	12
3.4 PARA LAS RA QUE HAN COMPARTIDO ENTORNO DE APLICACIÓN, APLICARÁ, ADEMÁS DE LAS EXIGENCIAS DEL ITEM 3.2, TAMBIÉN LOS SIGUIENTES REQUISITOS DE SEGURIDAD:	13
3.5 CONTROL POR CIRCUITO CERRADO DE TELEVISIÓN.....	13
3.6 PUESTOS PROVISORIOS INSTALADOS EN FERIAS O EVENTOS DE CORTA DURACIÓN	13
3.7 VALIDACIÓN DE SOLICITUD DE CERTIFICADOS EN AMBIENTES EXTERNOS A LA RA.....	13
4.1. ESTACIONES DE TRABAJO.....	14
4.2. APLICATIVO DE LA RA.....	15
5. SEGURIDAD DE REDES.....	17
6. SEGURIDAD DE LA INFORMACIÓN	17
6.1. DIRECTRICES GENERALES	17
6.2. ALMACENAMIENTO, MANIPULACIÓN, ARCHIVADO Y DESTRUCCIÓN DE DOCUMENTOS.....	18
7. CICLO DE VIDA DEL CERTIFICADO.....	20
7.1. PROCESOS DEL CICLO DE VIDA DEL CERTIFICADO.....	20
7.2. VALIDACIÓN ADICIONAL.....	20
8. ACUERDOS DE FUNCIONAMIENTO	21



<p style="text-align: center;">MINISTERIO DE INDUSTRIA Y COMERCIO</p> 	<p>Dirección General de Firma Digital y Comercio Electrónico</p>	<p>Página 4</p>
	<p>Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay</p>	<p>Anexo de la Resolución N° <u>1399</u></p>

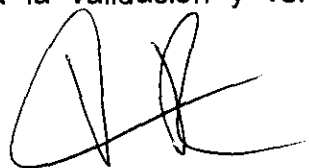
1. DISPOSICIONES GENERALES


1.1. Este documento tiene por objeto regular los procedimientos mínimos que deben ser adoptados por las Autoridades de Registro que operan en el marco de la Infraestructura de Claves públicas del Paraguay.

1.2. Estas normas se aplican a todas las RA y deben ser aplicadas en todas sus instalaciones técnicas y puestos provisorios. En el caso que exista procedimientos que deberán ser aplicados específicamente para un solo tipo de instalación, se indicará este hecho.

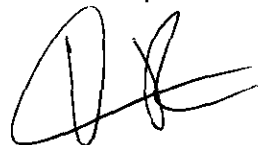
1.3. Para este documento, se aplican los siguientes conceptos:


- a) **Autoridad de Aplicación:** se designa al Ministerio de Industria y Comercio como órgano regulador competente por Ley, establecido por el artículo 38 de la Ley 4610/2012 que modifica y amplía la Ley N° 4017/2010 "De validez jurídica de la Firma Electrónica, Firma Digital, los Mensajes de Datos y el Expediente Electrónico". Ejerce funciones a través de su unidad administrativa, la Dirección General de Firma Digital y Comercio Electrónico, dependiente del Viceministerio de Comercio.
- b) **Autoridad de Certificación (CA):** entidad que presta servicios de emisión, gestión, revocación u otros servicios inherentes a la certificación digital. En el marco de la PKI Paraguay, son Autoridades de Certificación, la CA Raíz del Paraguay y el PSC.
- c) **Autoridad Certificadora Raíz o Autoridad de Certificación Raíz (CA Raíz):** es el órgano técnico dentro de la PKI, cuya función principal es habilitar al PSC y emitir a éste, el certificado digital correspondiente. Posee un certificado autofirmado y es a partir de allí, donde comienza la cadena de confianza.
- d) **Agente de Registro:** persona responsable de la ejecución de actividades relacionadas con la RA, que realiza la validación y verificación de la solicitud de certificado.




MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Pagina 5
	Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay	Anexo de la Resolución Nº <u>1399</u> -

- e) **Autoridad de Registro (RA):** entidad responsable de la identificación y autenticación de titulares de certificados digitales; la misma no emite ni firma certificados. Una RA interviene en el proceso de solicitud del certificado, en el proceso de revocación o en ambos. La RA, no necesita ser un organismo separado, sino que puede ser parte de la CA.
- f) **Dossier de Agente de Registro:** conjunto de documentos relativos al Agente de Registro: comprobante de profesión, comprobante de residencia, comprobantes de entrenamientos realizados, comprobante de verificación de antecedentes penales, y otros mencionados en el ítems 2.2.1 y 2.2.2 de este documento.
- g) **Dossier de instalación técnica:** conjunto de documentos relativos a la instalación técnica: Plan de Continuidad de Negocio, Análisis de Riesgos y otros mencionados en el ítem 6.1.2 de este documento.
- h) **Dossier titular del certificado:** conjunto formado por la copia del documento de identificación utilizados para emitir el certificado, la solicitud de emisión de certificado, el acuerdo de suscriptores, y la solicitud de revocación de certificado, en su caso.
- i) **Emisión del certificado:** comprende la generación del certificado, cuyo proceso es una función de la CA.
- j) **Infraestructura de Claves Públicas del Paraguay (PKI Paraguay):** es un conjunto de personas, políticas, procedimientos y sistemas informáticos necesarios para proporcionar servicios de autenticación, integridad y no repudio, mediante el uso de criptografía de claves públicas y privadas y de certificados digitales, así como la publicación de información, consulta de vigencia y validez de los mismos.
- k) **Instalación técnica:** ambiente físico de una RA, cuya operación fue debidamente autorizado por el Ministerio de Industria y Comercio, donde se realizan las actividades de validación y verificación de la solicitud de certificado. No posee un periodo de tiempo determinado para su funcionamiento.



MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Pagina 6
	Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay	Anexo de la Resolución N° <u>1399</u> -

- l) **La confirmación de la identidad de un individuo:** es la comprobación de que la persona que se presenta como el titular o responsable del certificado o como el representante legal de una persona jurídica, es realmente aquella cuyos datos están contenidos en la documentación presentada.
- m) **La confirmación de la identidad de una organización:** es la comprobación de que los documentos presentados se refieren efectivamente a la persona jurídica titular del certificado y que la persona que se presenta como el representante legal de la persona jurídica realmente tiene tal atribución.
- n) **La desvinculación de un Agente de Registro:** se produce en los siguientes casos:
- I. Cuando un empleado o funcionario que cumple el rol de Agente de Registro es desvinculado de la organización;
 - II. Cuando un empleado o funcionario que cumple el rol de Agente de Registro deja de ejercer de forma permanente el mencionado rol, incluso aunque continúe trabajando en la organización, en la instalación técnica o puesto provisorio de la RA.
- o) **Punto central del PSC:** local único en el territorio nacional, donde el PSC almacena copias del dossier de todos los Agentes de Registro de las RA vinculadas y pueden almacenarse también el dossier de los titulares de certificados de la PKI Paraguay.
- p) **Punto central de la RA:** local único en el territorio nacional donde la RA almacena el dossier de todos los Agentes de Registro. Pueden almacenarse también el dossier de los titulares de certificados de la PKI Paraguay.
- q) **Puesto provisorio:** ambiente montado por la RA, fuera de sus instalaciones técnicas, para la realización de actividades inherentes a las autoridades de registro. Posee un periodo de tiempo determinado para su funcionamiento.

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Pagina 7
	Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay	Anexo de la Resolución Nº <u>1399</u> -

- r) **Prestador de Servicios de Certificación:** entidad habilitada por la AA, encargada de operar una CA en el marco de la PKI Paraguay. El PSC debe contar con un certificado digital emitido por la CA Raíz del Paraguay y solo podrá emitir certificados a usuarios finales.
- s) **Suspensión del Agente de Registro:** se produce cuando un Agente de Registro deja de ejercer su rol de forma temporal. La suspensión solo implica la modificación de permisos del Agente de Registro en el sistema del PSC.
- t) **Validación de solicitud de certificado:** comprende las etapas de confirmación de la identidad de un individuo o una organización, realizada mediante la presencia física del interesado, sobre la base de los documentos de identificación, y la de emisión del certificado.
- u) **Verificación de solicitud de certificado:** confirmación de la validación de una solicitud de certificado.

1.4 Sólo podrán expedir certificados, las autoridades de registro que integran la PKI Paraguay que se encuentran debidamente habilitados por el Ministerio de Industria y Comercio, utilizando el equipo y/o puestos de trabajo temporal autorizados.


1.5 En caso de cambio de dirección de instalación técnica, el hecho debe ser previamente reportado al PSC responsable. Este enviará una solicitud de habilitación con los datos actualizados, solicitando una nueva autorización de funcionamiento a la CA Raíz.

1.6 Está prohibida la alteración de la dirección del puesto provisorio de la RA después de la autorización de su funcionamiento como tal.

1.7 El cumplimiento de las normas en este documento será verificado por auditorías e inspecciones llevadas a cabo por la CA Raíz o entidad autorizada por este.


 Abog. Borjys Rolón A.
 DIRECTOR GENERAL
 Firma Digital Comercio Electrónico



MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Pagina 8
	Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay	Anexo de la Resolución N° <u>1399</u> -

2. SEGURIDAD PERSONAL

2.1. DISPOSICIONES GENERALES

2.1.1. Las regulaciones que se refieren a la seguridad de las personas, están en el ítem 5.3 del documento **Directivas Obligatorias para la Formulación y Elaboración de la Práctica de Certificación de los Prestadores de Servicios de Certificación (PSC)**.

2.1.2 No se admiten funcionarios o empleados subcontratados en el ejercicio de actividades del Agente de Registro; quienes deben ser empleados o funcionarios de la propia organización habilitada como RA por la CA Raíz.

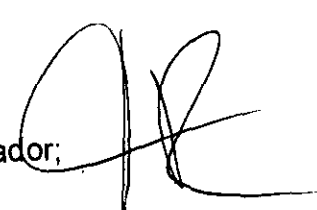
2.1.3 Puede ser firmado un acuerdo documentado, entre PSC y RA, en el cual el PSC responsable delega a la RA la actividad de incluir/excluir Agentes de Registros en el aplicativo de la RA. En este caso, el responsable por esta actividad, en la RA, debe ser formalmente designado.


2.1.4 La RA debe enviar al PSC la lista actualizada de los Agentes de Registros en actividad, sus perfiles cualificados y sus necesidades de acceso a informaciones del gerenciamiento del ciclo la vida de los certificados. El PSC debe mantener esas informaciones actualizadas, organizadas y consolidadas en su instalación técnica, inclusive con un histórico de las alteraciones realizadas, a disposición de la CA Raíz para los procedimientos de auditoría e inspección.

2.2. DOCUMENTACIÓN DEL AGENTE DE REGISTRO

2.2.1. Cada Agente de Registro que está actuando o que ha servido en la RA debe tener un dossier que incluya:

- a) Contrato de trabajo, donde consta los términos de la contratación y la función que cumple en la organización;
- b) Comprobante de verificación de antecedentes penales;
- c) Comprobante de verificación de histórico de empleos anteriores;
- d) Comprobante de profesión y de residencia;
- e) Comprobante de entrenamiento realizado;
- f) Resultado de la entrevista inicial con la firma del entrevistador;

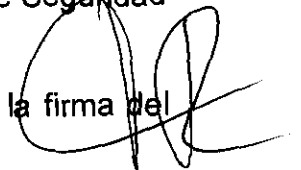



MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Pagina 9
	Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay	Anexo de la Resolución N° <u>1399</u> -

- g) Declaración en la que afirma conocer sus atribuciones y que asume el deber de cumplir con la Política de Seguridad del PSC responsable, las políticas y reglas establecidas por la CA Raíz y la normativa que rige la materia. En esta declaración asume también el deber de mantener la confidencialidad y exclusividad de la información proporcionada por el PSC a la RA y mantenerlo en secreto, incluso cuando se desvincula de la RA, respecto a todas las informaciones y los procesos ejecutados en la RA;
- h) Resultado de la revisión periódica prevista en la Política de Seguridad del PSC;
- i) Copia del documento, generado en medios digitales o en papel, que compruebe que la RA realizó (en los casos previstos en el punto 2.1.3) la solicitud al PSC para la habilitación del Agente Registro en el sistema de certificación;
- j) La confirmación de la CA a la RA (en los casos previstos en el punto 2.1.3), relativa a la inclusión de Agente de Registro en su sistema de certificación.

2.2.2. Si el Agente de Registro se ha desvinculado de sus actividades en la RA, el expediente debe también contener:

- a) Copia del documento, generado en medios digitales o en papel, que compruebe que la RA realizó (en los casos previstos en el punto 2.1.3) la solicitud al PSC de la desvinculación del Agente de Registro en el sistema de certificación;
- b) La confirmación del PSC a la RA (en los casos previstos en el punto 2.1.3) cuando ha desvinculado al Agente de Registro en el sistema de certificación;
- c) Una declaración firmada por el Agente de Registro, donde manifieste que no tiene asuntos pendientes, como los previstos en la Política de Seguridad del PSC referentes a seguridad del personal; y
- d) Resultado de la entrevista de desvinculación del personal con la firma del entrevistador;



MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Pagina 10
	Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay	Anexo de la Resolución N° _____

2.2.3 Los documentos 2.2.1.a al 2.2.1.h, que constituyen el dossier, deben ser examinados por una de las siguientes personas, que declaran, bajo pena de la normativa, la existencia de tales documentos y que estos documentos comprueban efectivamente que el Agente de Registro cumple con todos los requisitos relevante de la PKI Paraguay:

- a) Auditor Interno de la RA, inscripto ante la CA Raíz
- b) Auditor externo independiente inscripto ante la CA Raíz
- c) Auditor o funcionario designado por el PSC a la que está vinculada la RA inscripto ante la CA Raíz ;
- d) Representante legal propio de la RA.


2.2.4 Sólo después de la solicitud de vinculación del Agente de Registro y la declaración prevista en el punto anterior, el PSC o RA (en los casos previstos en el punto 2.1.3) puede incluirlo en la bases de datos y concederle los permisos de acceso en el sistema de certificación, siendo necesario para ello, la previa autorización documentada del Gerente del PSC o del responsable por el designado.

2.2.5. Los dossiers de todos los Agentes de Registros de una RA deben permanecer en un mismo punto centralizado en la RA, que será informado al PSC al cual está vinculada la RA.

2.3 ENTRENAMIENTO DEL AGENTE DE REGISTRO

2.3.1 Todo Agente de Registro, en el momento de la admisión, debe recibir entrenamiento o capacitación documentado, con una carga horaria mínima de 16 horas, sobre los siguientes temas:

- a) Principios y mecanismos de seguridad de la RA;
- b) Sistema de certificación en el uso de una CA;
- c) Procedimientos de recuperación de desastres y continuidad del negocio;
- d) Reconocimiento de firmas y validez de los documentos presentados;
- e) Otros asuntos relacionados con las actividades bajo su responsabilidad.

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Pagina 11
	Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay	Anexo de la Resolución N° <u>1399</u> -

2.3.2 En la formación sobre principios y mecanismos de seguridad deben ser presentadas en la Política de Seguridad del PSC, sus normas y procedimientos relativos al tratamiento de informaciones y/o los datos sensibles, con el fin de desarrollar y mantener una efectiva concienciación sobre la seguridad, así como instruir a su fiel cumplimiento.

2.3.3. El entrenamiento en el reconocimiento de firmas y la validez de los documentos, deberá ser suministrado (o preparado, cuando se trata de entrenamientos tipo e-learning) por la empresa o profesional especializado en grafotecnia.

2.4. ACOMPAÑAMIENTO PERIÓDICO

2.4.1. La RA debe acompañar el desempeño de las funciones de sus Agentes de Registro y evaluarlos anualmente con el propósito de detectar las necesidades de actualización técnica y de seguridad. Este proceso debe ser documentado.


2.4.2. La RA deberá exigir y verificar la renovación de los antecedentes penales de todos sus Agentes de Registros con una frecuencia de 2 años.

2.4.3. Para los casos en que el acompañamiento anual advierta la necesidad de suspender o desvincular a un Agente de Registro, dicha situación deberá ser inmediatamente solicitada al PSC o efectuada por la RA, según sea el caso.

2.4.4. La RA debe archivar los comprobantes relativos a los procedimientos anteriores en el dossier de los Agentes de Registro que obran en su poder.

2.5. SUSPENSIÓN Y TERMINACIÓN

2.5.1. Cuando el Agente de Registro es suspendido o desvinculado de sus actividades, la RA inmediatamente diligenciará la revocación de sus permisos de acceso al sistema de certificación del PSC y de acceso físico y lógico a los equipamientos y mecanismos inherentes a la actividad de Agente de Registro. Estos procesos serán documentados y archivados en el dossier del Agente de Registro y en poder de la RA.

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Pagina 12
	Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay	Anexo de la Resolución Nº <u>1399</u> -

2.5.2. La RA realiza (en los casos previstos en el punto 2.1.3) la solicitud al PSC de la revocación de los permisos de acceso al sistema de certificación, informando el motivo de la suspensión o desvinculación del Agente de Registro. El responsable designado para esa tarea expide la orden de revocación de permiso de acceso al sistema. Estos procesos serán documentados y archivados en copia en el dossier del Agente de Registro.

3. SEGURIDAD FÍSICA

3.1 LAS INSTALACIONES TÉCNICAS Y LOS PUESTOS TEMPORALES DE UNA RA PUEDEN SER DE 2 TIPOS:

- a) Ambiente dedicado a las actividades de la RA;
- b) Ambiente compartido con otras actividades de la organización.

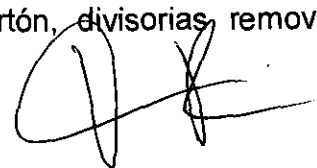
3.2 EN AMBOS CASOS, SE APLICAN LOS SIGUIENTES REQUISITOS MÍNIMOS DE SEGURIDAD:


- a) Equipos de prevención de incendios;
- b) Armario o gabinete con llave, de uso exclusivo de la RA, para mantener los documentos de la RA
- c) Los circuitos eléctricos de alimentación del equipo de procesamiento de datos serán protegidos por UPS o estabilizadores de tensión.
- d) Los circuitos eléctricos y lógicos deberán ser protegidos por cañerías y/o canaletas apropiadas.

3.3 PARA LAS RA QUE TENGAN UN ENTORNO DEDICADO, APLICARÁ, ADEMÁS DE LAS EXIGENCIAS DEL ÍTEM 3.2, TAMBIÉN LOS SIGUIENTES REQUISITOS DE SEGURIDAD:

- a) Revisión del control de acceso del ambiente dedicado, con autorización de acceso, sólo para los agentes de registros y titulares de certificados;
- b) Puerta de entrada única con cerradura reforzada;
- c) Paredes y techos que prevengan el acceso no autorizado, construidas de material cosido, paneles de yeso con cartón, divisorias removibles o material de resistencia equivalente;

Abog. Rodys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico



MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Pagina 13
	Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay	Anexo de la Resolución N° <u>1399</u> -

d) Iluminación de emergencia.

OBS: Si la habitación tiene ventanas o cualquier otra abertura al entorno exterior del edificio, estos deberán sellarse o ser enrejadas, para evitar el acceso externo.

3.4 PARA LAS RA QUE HAN COMPARTIDO ENTORNO DE APLICACIÓN, APLICARÁ, ADEMÁS DE LAS EXIGENCIAS DEL ITEM 3.2, TAMBIÉN LOS SIGUIENTES REQUISITOS DE SEGURIDAD:

- a) Vigilancia intensiva o monitoreo por circuito cerrado de televisión en el entorno de la RA;
- b) Control de acceso al edificio o al entorno en el que está instalada la RA.

3.5 CONTROL POR CIRCUITO CERRADO DE TELEVISIÓN

3.5.1. El control por circuito cerrado de televisión puede ser llevado a cabo por la propia RA o por la compañía de seguridad contratada. La cámara debe filmar el ambiente y el equipamiento de la RA y las imágenes deben ser mantenidas por 60 días en un ambiente seguro.

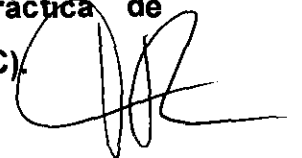
3.6 PUESTOS PROVISORIOS INSTALADOS EN FERIAS O EVENTOS DE CORTA DURACIÓN


3.6.1 Para los casos específicos de los puestos provisorios de RA instalados en ferias y eventos con un periodo de funcionamiento máximo de 15 días, están exentas las exigencias de seguridad establecidas en el ítem 3.4. Están también exentas las exigencias de seguridad establecidas en el ítem 3.2, desde que los documentos y equipamientos sean llevados para su almacenamiento en una instalación técnica de la RA, al cierre diario de las actividades del puesto provisorio.

3.7 VALIDACIÓN DE SOLICITUD DE CERTIFICADOS EN AMBIENTES EXTERNOS A LA RA

3.7.1. Las actividades de la RA relativas a la validación de la solicitud de certificados pueden ser ejecutadas externamente al ambiente de la RA, siempre y cuando se cumplan con las disposiciones establecidas ítem 3 de las **Directivas Obligatorias para la Formulación y Elaboración de la Práctica de Certificación de los Prestadores de Servicios de Certificación (PSC)**.

Abog. Rodrys Rolón A.
DIRECTOR GENERAL
Firma Digital y Comercio Electrónico



MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Pagina 14
	Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay	Anexo de la Resolución Nº <u>1309</u> -

3.7.2. La RA sólo puede utilizar la modalidad de validación externa, después de adaptar sus equipos móviles a los dispuesto en el ítem 4.1.2 de este documento y desde que la CA al cual la RA se vincula, tenga adaptados sus procedimientos, su sistema de certificación y/o aplicación de RA con todas las normas establecidas en este documento y las disposiciones establecidas en el punto 3.b. de las **Directivas Obligatorias para la Formulación y Elaboración de la Práctica de Certificación de los Prestadores de Servicios de Certificación (PSC)**

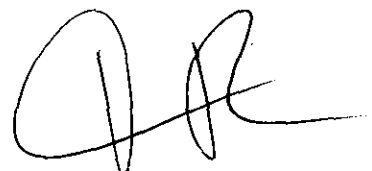
4. SEGURIDAD LÓGICA


4.1. ESTACIONES DE TRABAJO

4.1.1. Las estaciones de trabajo de la RA, incluidos los equipamientos portátiles deben ser protegidos frente a amenazas y acciones no autorizadas, así como contra el acceso no autorizado, y del uso o la exposición indebida.

4.1.2. Las estaciones de trabajo de la RA, incluidos los equipamientos portátiles, deben recibir, por lo menos, las siguientes configuraciones de seguridad:

- a) Control de acceso lógico al sistema operativo;
- b) La exigencia de utilizar contraseñas fuertes y seguras;
- c) Políticas de contraseñas y bloqueo de cuentas;
- d) Logs de auditoría del sistema operativo activo que registre:
 - i. Inicio y apagado del sistema;
 - ii. Intentos de crear, eliminar, establecer contraseñas o cambiar los privilegios de los sistemas de operaciones de la RA;
 - iii. Cambios en la configuración de la estación;
 - iv. Intentos de acceso (login) y de salida del sistema (logoff);
 - v. Intentos no autorizados de acceso a los archivos del sistema;
 - vi. Intentos de iniciar, eliminar, habilitar y deshabilitar a los usuarios y de actualizar y recuperar sus claves.
- e) Poseer antivirus, antispyware y anti troyano, instalados, actualizados y habilitados;



MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Pagina 15
	Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay	Anexo de la Resolución N° <u>1399</u> -

- f) Firewall personal activado, con permisos de acceso mínimo necesarios para las actividades. Este requerimiento puede ser sustituido por firewall corporativo, para los equipos instalados en redes que tienen tal dispositivo;
- g) Protector de pantalla accionado como máximo 2(dos) minutos de inactividad y exigiendo para su desbloqueo la contraseña del usuario;
- h) Sistema operativo actualizado, con la aplicación de las correcciones necesarias (patches, hotfix, etc) ;
- i) Utilizar solamente software con licencias y solamente aquellos necesarios para llevar a cabo las actividades del usuario;
- j) Impedimento de acceso remoto, a través de otro equipo conectado a la red utilizado por la RA, excepto para las actividades de soporte remoto;
- k) Utilización de fecha y hora legal paraguaya.

4.1.3 Los logs de auditoría del sistema operativo deben registrar los accesos a los equipos y deben ser almacenados localmente por un período mínimo de 60 días.

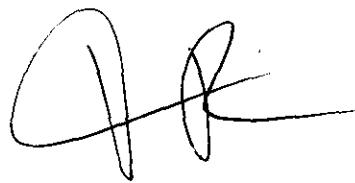
4.1.4 El análisis de los disser de los logs solamente se llevará a cabo en caso de sospecha de acceso no autorizado o dar respuestas a otras preguntas que surgen de la utilización de equipos.


4.1.5 Es deseable que el Agente de Registro no posea el perfil de administrador o contraseña de root de los equipos, dejando esa tarea delegada a terceros de la propia organización, a fin de permitir la segregación de funciones.

4.2. APLICATIVO DE LA RA

4.2.1. El aplicativo que hace de interfaz entre la RA y el sistema de certificación de la CA debe poseer por los menos las siguientes características de seguridad:

- a) Acceso permitido solamente mediante autenticación por medio de certificado de tipo F2 del Agente de Registro.
- b) Acceso permitido únicamente a dispositivos autenticados en el sistema (por ejemplo: usando registro previo de la dirección IP, certificado digital del equipo u otra solución que permita al sistema identificar de forma inequívoca al equipo) ;




MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Pagina 16
	Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay	Anexo de la Resolución N° 1399

- c) Timeout de sesión de acuerdo con el análisis de riesgo de la CA;
- d) Registro en logs de auditorías de los eventos mencionados en el ítem 5.4.1. de las **Directivas Obligatorias para la Formulación y Elaboración de la Práctica de Certificación de los Prestadores de Servicios de Certificación (PSC)**
- e) Histórico de inclusión y exclusión de los Agentes de Registro en el sistema y de los permisos concedidos o revocados;
- f) Registro en logs, para cada certificado emitido, indicando si la validación de solicitud del certificado se realizó internamente o externamente al ambiente de la RA;
- g) Mecanismo de revocación inmediata de certificados digitales emitidos fuera del ambiente de la RA y que no han sido verificadas por un segundo Agente de Registro, mediante la copia de la documentación en la etapa de validación, hasta el momento de inicio de validez del certificado.

4.2.2 Para el cumplimiento de lo dispuesto en el ítem 6.1 de las **Directivas Obligatorias para la Formulación y Elaboración de la Práctica de Certificación de los Prestadores de Servicios de Certificación (PSC)**, la aplicación debe:

- a) Haber sido desarrollado con documentación formal;
- b) Contar con mecanismos de control de versiones;
- c) Tener la documentación de pruebas realizadas a cada versión;
- d) Poseer documentación que evidencie la homologación de cada versión en un ambiente con las mismas características al que se presentará cuando sea utilizado en producción, siendo estos ambientes obligatoriamente separados unos de otros;
- e) Tener la aprobación documentada del gerente o el responsable designado de la CA al cual está vinculada la RA, para instalar cada versión a un ambiente de producción.



MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Pagina 17
	Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay	Anexo de la Resolución Nº <u>1399-</u>

OBS: Sólo para las versiones de aplicaciones de RA que estuvieren en producción, a la fecha de publicación de esta declaración, estarán exentas del cumplimiento de los ítem c, d y e.

4.2.3. Los logs generados por este aplicativo deben ser almacenados en la CA al cual está vinculada la RA, por un período de diez años, conforme a lo dispuesto en el ítem 5.5.2 de las **Directivas Obligatorias para la Formulación y Elaboración de la Práctica de Certificación de los Prestadores de Servicios de Certificación (PSC)**.

5. SEGURIDAD DE REDES

5.1. Cada instalación técnica o puesto provisorio de la RA que tenga que operar por un plazo mayor a 15 días, deberá elaborar el diagrama de la topología de la red de comunicación entre la RA y el PSC al cual está vinculada, que deberán mantenerse siempre actualizada. Este documento debe ser archivado en el dossier de la instalación técnica o puesto provisorio.

5.2. La RA remitirá las solicitudes de emisión o revocación de certificados al PSC utilizando un VPN (Virtual Private Network - red privada virtual), SSL (capa de conexión Segura - protocolo de comunicación seguro) u otra tecnología de igual o mayor nivel de seguridad y privacidad.

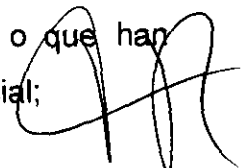
6. SEGURIDAD DE LA INFORMACIÓN


6.1. DIRECTRICES GENERALES

6.1.1 Todas las informaciones y documentaciones de la instalación técnica o puesto provisorio de la RA deberán ser clasificadas y almacenadas conforme a los requisitos de seguridad compatibles con lo establecido en la Política de Seguridad de la Información del PSC a la cual está vinculada la RA.

6.1.2 Cada instalación técnica o puesto provisorio de la RA deberán poseer un dossier que contenga copias actualizadas de los siguientes documentos:

- a) Contrato de los Agentes de Registro que están trabajando o que han trabajado en la RA con sus respectivos números de cédula policial;



MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Pagina 18 Anexo de la Resolución N° <u>1399</u> -
	Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay	

- b) Topología de red de comunicación entre la RA y el PSC;
- c) Manual de operaciones del Agente de Registro;
- d) Inventario de activos de la información;
- e) Plan de Continuidad del Negocio;
- f) Análisis de Riesgos.

6.1.3 El Análisis de Riesgo y Plan de Continuidad del Negocio deben elaborarse de acuerdo con lo dispuesto en la Política de Seguridad de la Información del PSC.

6.1.4. Para los casos específicos de los puestos provisorios instalados en las ferias y eventos con un período de funcionamiento no mayor 15 días, estará exenta de la elaboración del Análisis de Riesgo y el Plan de Continuidad de Negocio.

6.1.5 Una copia de la Plan de Continuidad del Negocio debe ser almacenado en un lugar seguro, fuera de las instalaciones de la RA.


6.1.6 El inventario de activos de la información debe estar siempre actualizado, manteniendo un histórico de los cambios y debe ser firmado por la persona responsable de la instalación técnica o puesto provisorio.

6.1.7 El inventario de los bienes debe indicar al menos:

- a) Los equipos de la RA, con sus respectivas especificaciones, actualizados mensualmente;
- b) El software instalado en los equipos, actualizado mensualmente;
- c) Valoración de los activos en cuando a Integridad, confidencialidad y disponibilidad.

6.2. ALMACENAMIENTO, MANIPULACIÓN, ARCHIVADO Y DESTRUCCIÓN DE DOCUMENTOS.

6.2.1 Los documentos en papel que componen el dossier de los titulares de certificados y de la instalación técnica o puesto provisorio, deben ser guardados, obligatoriamente, en un armario con cerradura, con acceso permitido sólo a los Agentes de Registro.

MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Pagina 19
	Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay	Anexo de la Resolución Nº <u>1399</u> -

6.2.2 La RA puede sustituir la custodia física de los documentos que integran el dossier del Agente de Registro y el dossier del titular del certificado mediante la reproducción digital de los mismos, siempre que:


- a) Los documentos cuyas copias debe constar en el dossier (por ejemplo: documentos de identidad presentada por el titular, etc.) sean escaneados y firmados digitalmente con el certificado de firma digital.
- b) Los documentos cuyo original debe constar en el dossier (por ejemplo: Solicitud de Certificados, Acuerdos de suscriptores, Contrato de Agente de Registro, etc.), pueden ser reproducidos y almacenados electrónicamente conforme a lo establecido en la Ley N° 4017/2010 y sus reglamentaciones, o en formato papel. Los mismos deberán permanecer archivados en la instalación central de la RA en el plazo establecido en las normativas de la PKI Paraguay.
- c) Todos los archivos que componen un dossier deben ser organizados para permitir su recuperación conjunta con fines de inspección y auditoría;
- d) El directorio del sistema donde son almacenados esos archivos deben tener protección contra lectura y escritura, dando permiso de acceso sólo a los Agentes de Registro o al responsable designado formalmente para trabajar con esos documentos;
- e) Deben ser especificados procedimientos de copias y recuperación en el caso de un siniestro.

6.2.3. El almacenamiento definitivo de los dossiers de titulares de certificados en papel, digitalizado, se debe hacer:

- a) En uno de los puntos de las instalaciones de la RA, para aquellos que tienen más de una instalación técnica; o
- b) En el punto central del PSC a la que está vinculada la RA.

6.2.4 A criterio de cada RA, puede ser mantenida una copia del dossier en la instalación técnica o puesto provisorio en la que fue generado, y que no sustituye el almacenamiento original en los locales antes citado.



MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Pagina 20
	Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay	Anexo de la Resolución N° <u>1399</u>

6.2.5 El envío o transmisión del dossier para el almacenamiento definitivo deben estar realizado por un medio seguro (por ejemplo: entrega con acuse de recibo de los documentos en papel y la transmisión a través de VPN para los documentos digitalizados), dentro de los 30 días corridos, desde la generación del dossier.

6.2.6. La RA debe utilizar el sistema en el que se pueda determinar, fácilmente y en cualquier momento, la ubicación en el cual se encuentra cada dossier del titular del certificado que está bajo su cuidado.

6.2.7 El punto centralizado del PSC y/o el punto centralizado de la RA debe poseer requisitos de seguridad física y/o lógica, al menos, equivalentes a la instalación técnica de la RA y su ubicación debe ser comunicado al Ministerio de Industria y Comercio, así como cualquier cambio que se realizare posteriormente.

6.2.8. Todos los documentos en papel que contienen información clasificada como sensible deben ser destruidos, de forma que sea irrecuperable la información contenida, antes de ser desechadas. Se incluyen en esta categoría las copias de documentos de los titulares de los certificados, solicitud de emisión o revocación de certificados, acuerdos de suscriptores o diagramas de redes no utilizados, etc.

6.2. Cuando la eliminación de un archivo que contenga copias de documentos de dossier de titulares de certificados, la diligencia debe llevarse a cabo con la eliminación completa, incluyendo la limpieza de la papelera de reciclaje, de forma a impedir su recuperación y uso indebido.

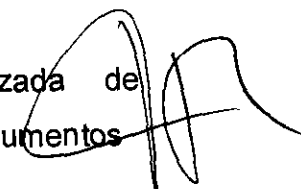
7. CICLO DE VIDA DEL CERTIFICADO


7.1. PROCESOS DEL CICLO DE VIDA DEL CERTIFICADO

7.1.1. Los procesos relativos al ciclo de vida del certificado: solicitud, validación y verificación de la solicitud, emisión y revocación, se describen en el ítem 4 del documento **Directivas Obligatorias para la Formulación y Elaboración de la Práctica de Certificación de los Prestadores de Servicios de Certificación (PSC)**.

7.2. VALIDACIÓN ADICIONAL

7.2.1. El PSC debe implementar cualquier forma sistematizada de consulta/validación de uno o más datos constante contenidos en los documentos



MINISTERIO DE INDUSTRIA Y COMERCIO 	Dirección General de Firma Digital y Comercio Electrónico	Pagina 21
	Características mínimas de seguridad para la Autoridades de Registro de la Infraestructura de Claves Públicas del Paraguay	Anexo de la Resolución N° <u>1399</u> -

de identidad presentado por el solicitante del certificado digital para fines de identificación, basado en las normas y reglas de los órganos emisores del documento de identidad, sin perjuicio de otras consultas obligatorias.

8. ACUERDOS DE FUNCIONAMIENTO

8.1. Según lo previsto en el ítem 1.3.2 de las **Directivas Obligatorias para la Formulación y Elaboración de la Práctica de Certificación de los Prestadores de Servicios de Certificación (PSC)**, el PSC habilitado por el Ministerio de Industria y Comercio podrá celebrar un contrato de acuerdo operacional, de modo a que las actividades asignadas a una RA, corran por cuenta de un tercero

Estos contratos deben tener al menos las siguientes cláusulas:

- a) Identificación de la RA y PSC;
- b) Identificación de las atribuciones que le tocará a cada uno de los intervinientes del contrato;
- c) La identificación del sitio y responsable de la custodia de los dosiers de los titulares de certificados, incluso en el caso de la terminación del contrato;
- d) El compromiso de que los celebrantes del mismo, se ajusten a cumplir con la Leyes y las Normas que rigen para la PKI Paraguay, en todos los procedimientos realizados;
- e) El período para el que se suscriba el contrato que no debe exceder al máximo previsto en el Código Civil Paraguayo, salvo que la actividad pueda enmarcarse dentro de las excepciones establecidas en el mismo cuerpo normativo señalado;
- f) Obligación del PSC contratista, de verificar el cumplimiento de los procesos ejecutados por la RA contratada.


 Abog. Rólys Rolón A.
 DIRECTOR GENERAL
 Firma Digital y Comercio Electrónico

