



Directrices para las Autoridades de Registro. Características de cumplimiento de Autoridades de Registro (RA) de la jerarquía nacional de certificadores registrados de Costa Rica

**Dirección de Certificadores de Firma Digital
Ministerio de Ciencia y Tecnología**



Control de versiones

Fecha	Versión	Autor(es)	Aprobado	Descripción
03-12-07	Borrador	Comité de Políticas	Lic.Oscar Solís Director DCFD	Se incorporan las observaciones de la consulta pública, de acuerdo al edicto publicado el día lunes 19 de noviembre del 2007 en el diario oficial "La Gaceta", número N° 222
04-09-08	1.00	Comité de Políticas	Lic.Oscar Solís Director DCFD	Oficialización y entrada en vigencia de las políticas.

Índice

1.	Disposiciones Generales.....	1
1.1	Administración del documento.....	3
1.1.1	Organización que administra el documento	3
1.1.2	Persona de contacto	3
2.	Controles del Personal	3
2.1	Disposiciones generales	3
2.2	Requerimientos de documentación del Agente de Registro	3
2.3	Requerimientos Capacitación	4
2.4	Procedimiento de suspensión o desvinculación.....	4
3.	Controles físicos	5
3.1	Exigencias mínimas de seguridad física.....	5
3.2	Procedimientos de monitoreo	5
4.	Controles lógicos	5
4.1	Controles de seguridad de las estaciones de trabajo.....	5
4.2	Controles de la aplicación de la RA.....	6
5.	Controles de seguridad de la RED.....	7
6.	Controles de seguridad de la información.....	8
6.1	Directrices generales.....	8
6.2	Procedimientos de almacenamiento, manipulación y destrucción de documentos	8
7.	Controles del ciclo de vida del certificado	9
8.	Acuerdos operacionales	9

1. Disposiciones Generales

Este documento regula la operación y procedimientos mínimos adoptados por las Autoridades de Registro (en adelante RA) que gestionan los certificados dentro de la jerarquía nacional de certificadores registrados de Costa Rica, y es un complemento de la “Política de Certificados para la jerarquía nacional de certificadores registrados”

La Autoridad de Registro (RA) es la entidad responsable por la comunicación entre el usuario y la autoridad certificadora (CA). Está vinculada a una CA y tiene por objetivo recibir, validar, verificar y gestionar las solicitudes de emisión o revocación de los certificados digitales, cumpliendo con lo establecido en la política de certificación nacional y en concordancia con las políticas y procedimientos definidos por la CA correspondiente

Para el presente documento se aplican las definiciones del “Reglamento a la Ley de certificados, firma digitales y documentos electrónicos (Decreto No. 33018-MICIT)” y de la “Política de Certificados para la jerarquía nacional de certificadores registrados”. Sin embargo, para ampliar la reglamentación de la RA se deben aclarar los siguientes conceptos:

- a. Agente de registro: Persona responsable de la ejecución de las actividades propias de la RA. Esta persona debe realizar las validaciones y verificaciones definidas en la política del certificado que corresponda.
- b. Confirmar la identidad del solicitante: proceso para comprobar que el solicitante es la persona con autoridad para solicitar el certificado, de acuerdo a la política asociada al certificado.
- c. Suspensión de un agente de registro: Es cuando un funcionario que tiene el rol de agente de registro deja de ejercer sus labores temporalmente, alterándosele sus permisos dentro del sistema de la CA.
- d. Desvincular a un Agente de Registro: Es el proceso de separar a un agente de registro de sus funciones, eliminándole los permisos dentro del sistema de la CA. Este proceso ocurre cuando:
 1. El funcionario ha renunciado a su cargo en la organización
 2. El funcionario es cesado de sus funciones o de su organización
 3. El funcionario que ha recibido la función de agente de registro la deja de ejercer, aunque continúa trabajando en otros puestos de la organización.
 4. El funcionario sancionado mediante un proceso administrativo, o por un procedimiento disciplinario, que impidan continuar en su cargo.
- e. Encargado de la RA: Persona responsable de la supervisión de las funciones de los agentes de registro, y la coordinación con la CA.

- f. Expediente del agente de registro: Es el conjunto de documentos relativos a un agente de registro.
- g. Expediente de instalación: Es el conjunto de documentos relativo a las instalaciones de la RA, tales como plan de continuidad de negocio, análisis de riesgos, reglamento de sanciones, inventario de activos y un plan de terminación de la RA (de acuerdo con el punto “5.8 Terminación de una CA o RA” del documento de Política de certificados para la jerarquía nacional de certificadores registrados).
- h. Instalaciones: Es el ambiente físico de una RA, cuyo funcionamiento es debidamente autorizado para realizar las actividades de validación y verificación de las solicitudes de certificado.
- i. Validación del solicitante del certificado: Es la verificación de la identidad del individuo o la organización que se presente ante una RA para solicitar un certificado. Esta validación requiere de la presencia física del solicitante y de la evidencia que permita determinar su autoridad para la solicitud de su certificado respectivo.

Las áreas y actividades ejecutadas por la RA incluyen, entre otras:

- › Verificar y validar los documentos de identidad
- › Registrar y enrolar a los suscriptores
- › Entregar certificados digitales
- › Gestionar la aceptación del certificado por parte del suscriptor
- › Gestionar revocaciones de certificados
- › Registrar los eventos en las bitácoras
- › Controlar y supervisar a los agentes de registro
- › Almacenar y custodiar la documentación
- › Controlar los reportes de incidentes
- › La RA debe establecer los procedimientos y guías para asegurar el cumplimiento de la política de certificados de la jerarquía nacional y de este documento, además de tomar las acciones que prevengan alguna deficiencia de la RA, incluyendo la terminación o suspensión de sus deberes.

1.1 Administración del documento

1.1.1 Organización que administra el documento

Dirección de Certificadores de Firma Digital

Ministerio de Ciencia y Tecnología, dirección: San José, 50 metros Este del Museo Nacional. Apartado Postal: 5589-1000 San José, Costa Rica. Correo Electrónico: informacion@firmadigital.go.cr

1.1.2 Persona de contacto

Jefatura de la Dirección de Certificadores de Firma Digital Director de Certificadores de Firma Digital, Correo Electrónico: informacion@firmadigital.go.cr. Tel. (506) 2248-1515

2. Controles del Personal

2.1 Disposiciones generales

La autoridad de registro es la responsable administrativa de su operación y debe enviar a la CA la información actualizada de los agentes de registros activos, sus perfiles, cualidades y necesidades de acceso a la información. Esta información es actualizada y consolidada por la CA, ejecutando los más estrictos procedimientos de custodia y fiscalización indicados en la sección 5.5.3 “protección de archivos”, de la Política de Certificados para la jerarquía nacional de certificadores registrados.

Los agentes de registro deben ser funcionarios de la organización que opera como Autoridad de Registro.

2.2 Requerimientos de documentación del Agente de Registro

Para cada agente de registro, en concordancia con los requisitos de personal ejecutando roles de confianza en la sección 5.3 de la política de certificados para la jerarquía nacional de certificadores registrados, la RA correspondiente debe poseer un expediente con:

- a. Un contrato de trabajo o documento que permita comprobar su situación laboral
- b. Comprobante de verificación de antecedentes criminales
- c. Comprobante de verificación de situación crediticia
- d. Comprobante de verificación de empleos anteriores. Incluyendo empleos en otras RA y las sanciones aplicadas, en caso de que existan.
- e. Comprobante de escolaridad y residencia

- f. Comprobante de aprobación de las capacitaciones recibidas referentes a las actividades propias de un Agente de Registro.
- g. Declaración en que afirma conocer las atribuciones que asume y el deber de cumplir con la política nacional de certificación, y de mantener confidencialidad y privacidad de los datos disponibles en la CA o RA
- h. Resultados de las evaluaciones periódicas
- i. Registro que lo compromete a ejecutar labores de agente de registro en la RA
- j. Registro en la CA o RA del momento en que fue incluido el rol de agente en el sistema de certificación

Cuando un Agente de Registro es desvinculado o suspendido de sus actividades en la RA entonces el expediente de la persona debe indicar:

- Registro de la solicitud para deshabilitar al agente de registro del sistema de certificación
- Registro en la CA del momento en que el agente de registro es deshabilitado o suspendido del sistema de certificación

2.3 Requerimientos Capacitación

Todo agente de registro, y personal involucrado de su administración, debe recibir capacitación y documentación en los siguientes temas:

- a. Concepto básico de certificados digitales, Tokens y Smart Card
- b. Principios y mecanismos de seguridad de la RA
- c. Uso del Sistema de Certificación de la CA
- d. Procedimientos de recuperación de desastres y de continuidad del negocio
- e. Procedimientos para la validación y verificación de identidad

Esto deberá constar en el expediente de agente de registro. Cuando se presenten cambios significativos en las operaciones de la RA, el personal involucrado debe recibir capacitación al respecto.

2.4 Procedimiento de suspensión o desvinculación

Cuando un Agente de Registro sea suspendido o desvinculado de sus actividades, el encargado de la RA debe gestionar inmediatamente con la CA la suspensión o revocación de sus permisos de acceso a los sistemas de la CA y de las labores inherentes a las actividades de la RA. Estos procesos deben ser documentados.

3. Controles físicos

3.1 Exigencias mínimas de seguridad física

Todas las Autoridades de Registro deben cumplir con las siguientes exigencias mínimas de seguridad:

- a. Dispositivos para la detección de incendios
- b. Gabinetes o armarios con llave, de uso exclusivo de la RA
- c. Los equipos de la RA deben estar protegidos contra fallas del fluido eléctrico y otras anomalías en la energía
- d. Vigilancia y monitoreo del ambiente de la RA durante su horario de operación
- e. Un perímetro de seguridad en el edificio donde se encuentran las instalaciones de la RA, con un guarda asignado durante el horario de operación.
- f. Controles contra coacción para cada agente de registro
- g. Iluminación de emergencia

3.2 Procedimientos de monitoreo

Mantener monitoreo por Circuito Cerrado de Televisión (CCTV), o cualquier otra tecnología de video-vigilancia, para la supervisión de las actividades de la RA. Las imágenes deben ser mantenidas en un ambiente seguro por al menos 60 días.

4. Controles lógicos

4.1 Controles de seguridad de las estaciones de trabajo

Las estaciones de trabajo de la RA, incluyendo los equipos portátiles, deben estar protegidas contra amenazas y acciones no autorizadas.

Las estaciones de trabajo de la RA, deben cumplir las siguientes directivas de seguridad:

- a. Control de acceso lógico al sistema operacional
- b. Autenticación robusta (por ejemplo, utilizando certificados digitales) para hacer uso de las estaciones de trabajo
- c. Directivas bloqueo de la sesión de usuario
- d. Bitácoras de auditoría del sistema operativo activadas, registrando:
 1. Inicio y terminación de las sesiones del sistema operativo

2. Intentos de crear, remover, definir contraseñas o modificar los privilegios del sistema operativo
 3. Modificaciones en la configuración de las estaciones
 4. Accesos (login) y de salidas (logoff) del sistema operativo
 5. Intentos de acceso no autorizado al sistema operativo
- e. Antivirus instalados, actualizados y habilitados
 - f. Permisos de acceso mínimos que le permitan ejecutar las actividades estrictamente necesarias.
 - g. Protector de pantalla activado como máximo dos minutos después de estar en inactividad el equipo y exigiendo un mecanismo de autenticación del usuario para desbloquearlo.
 - h. Sistema operativo actualizado y con la aplicación de las correcciones necesarias (parches, hotfix, etc.)
 - i. Endurecimiento de Estación (Hardening¹)
 - j. Instalar únicamente aplicaciones autorizadas y concernientes a la función.
 - k. Utilización de software licenciado en las estaciones de la RA
 - l. Limitar el acceso remoto a la estación de trabajo de la RA, vía otro equipo ligado a una red de computadores utilizada por la RA, excepto para actividades de soporte remoto de la CA
 - m. Sincronización con la hora UTC en Costa Rica

Las bitácoras deben permanecer almacenadas localmente por un periodo de al menos 60 días y posteriormente pueden ser eliminadas.

En las estaciones de la RA debe contarse con un perfil de administrador de los equipos, que sea el responsable de administrar la configuración de la máquina y esta labor debe ser segregada de las funciones del agente de registro de la RA.

4.2 Controles de la aplicación de la RA

La aplicación de la RA es la conexión entre la RA y el sistema de certificados de la CA y debe cumplir al menos con las siguientes funcionalidades:

- a. Autenticar robustamente (por ejemplo utilizando un certificado digital) al funcionario que funge en el rol de agente de registro

¹ El Hardening es una técnica compuesta por un conjunto de actividades llevadas a cabo por el administrador de un sistema operativo para reforzar al máximo posible la seguridad de este.

- b. Permitir acceso solamente a través de equipos autenticados
- c. Almacenar el historial de las inclusiones y exclusiones de los agentes de registro y los permisos o revocatorias aplicadas
- d. Proveer mecanismo de revocación automática de los certificados por parte del suscriptor o dueño del certificado
- e. Almacenar información que evidencie los procesos de identificación y autenticación de los solicitantes
- f. Implementar controles para verificar la información incluida en el certificado digital, en particular validarlos con las fuentes oficiales de información definidas en política de Certificados para la jerarquía nacional de certificadores registrados
- g. Remitir la solicitud de certificado digital a la CA emisora, firmada digitalmente
- h. Proveer métodos de activación de los dispositivos criptográficos a través de esquemas seguros, que evite divulgar información acerca de la activación de los dispositivos.
- i. Evidenciar que el proceso de generación e instalación del certificado se realizó dentro del tiempo definido en la sección “4.2.3 Tiempo para procesar solicitudes de certificado” de las políticas de certificación o con base en el acuerdo del suscriptor.
- j. Implementar controles para la preservación de la privacidad de la información
- k. Dejar evidencia para los certificados de persona física de la aceptación de los deberes y responsabilidades por parte del suscriptor acerca del uso del certificado, firmando digitalmente el comprobante de aceptación con el certificado entregado y validando que funciona correctamente
- l. Registrar en la bitácoras de auditoría las operaciones del ciclo de vida del certificado
- m. Reportar cualquier incidente a la CA

5. Controles de seguridad de la RED

Cada instalación de la RA debe mantener los componentes de su red local en un ambiente físicamente seguro y sus configuraciones deben ser revisadas periódicamente. Además, deben protegerse la privacidad e integridad de los datos sensibles.

6. Controles de seguridad de la información

6.1 Directrices generales

Toda la información y documentos relacionados con la instalación y puesta en operación de la RA deben ser clasificados y almacenados de acuerdo a los requisitos de seguridad definidos en la sección “5.5 Archivado de registros” de Política de certificados para la jerarquía nacional de certificadores registrados; y que garantizan privacidad y confidencialidad de la información.

El “Expediente de Instalación” es un documento clasificado como privado y confidencial, por mantener información sensible de la instalación técnica de la RA, y está constituido por los siguientes documentos actualizados:

- a. Plan de continuidad del negocio
- b. Análisis de riesgos
- c. Reglamento de sanciones
- d. Plan de terminación de una RA
- e. Inventario de Activos de la RA

Adicionalmente, debe tener disponible los siguientes documentos para uso de los agentes de registro:

- Copia de las políticas de certificación
- Manual de operación para los agentes de registro

6.2 Procedimientos de almacenamiento, manipulación y destrucción de documentos

Los documentos en papel que componen los expedientes de los solicitantes de certificado deben ser guardados obligatoriamente en archivos donde únicamente tengan acceso los agentes de registro. Una RA puede sustituir los documentos físicos por digitales, siempre y cuando estén firmados digitalmente con un certificado emitido por la jerarquía nacional de certificación digital.

Los documentos que contengan información confidencial o privada deben ser almacenados en los gabinetes o armarios con llave de uso exclusivo de la RA y cuando se dejen de utilizar deberán ser destruidos, de tal forma que no se pueda recuperar la información contenida en ellos.

7. Controles del ciclo de vida del certificado

La RA debe respetar el ciclo de vida del certificado definido en el capítulo 4 “Requerimientos operacionales del ciclo de vida del certificado”, del documento de “Política de certificados para la jerarquía nacional de certificadores registrados”.

8. Acuerdos operacionales

La CA debe celebrar un acuerdo operacional para que la RA ejecute las actividades de validación y verificación de las solicitudes de certificado. Este acuerdo debe contener al menos:

- a. La identificación y calidades de los celebrantes del acuerdo de la RA
- b. La identificación de los deberes que competen a la RA en función del acuerdo
- c. La identificación de los responsables de la RA
- d. Compromiso de la RA de cumplir con las normas y procedimientos definidos
- e. Plazo por medio del cual el acuerdo es celebrado
- f. Obligaciones de la RA para verificar los procesos que ejecuta