DIRECTRICES PARA LAS AUTORIDADES DE REGISTRO
Características de cumplimiento de Autoridades de Registro (RA) de la jerarquía nacional de certificadores registrados de Costa Rica.

Departamento de Certificadores de Firma Digital
Dirección de Gobernanza Digital
Ministerio de Ciencia, Tecnología y Telecomunicaciones

OID 2.16.188.1.1.1.1
Versión: 1.1
21 de Febrero, 2018


micitt
MINISTERIO
DE CIENCIA, TECNOLOGÍA
Y TELECOMUNICACIONES

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 Nº 222
04-09-08	1.00	Comité de Políticas	Lic. Oscar Solís Director DCFD	Oficialización y entrada en vigencia de las políticas**.**
14-09-17	Consulta pública (1.1)	Dirección de Certificadores de Firma Digital	Alexander Barquero Director DCFD	Actualizaciones para adoptar mejoras a la gestión de las RA.
08-09-17	Borrador	Dirección de Certificadores de Firma Digital	Alexander Barquero Director DCFD	Se incorporan las observaciones de la consulta pública.
21-02-18	1.1	Dirección de Gobernanza Digital (Departamento de Certificadores de Firma Digital)	Alexander Barquero Director DGD	Oficialización y entrada en vigencia de la versión 1.1 de las directrices.

Índice

1. Disposiciones Generales

Este documento regula la operación y procedimientos mínimos adoptados por las Autoridades de Registro (en adelante RA) que gestionan el proceso de emisión y/o revocación de los certificados digitales dentro de la Jerarquía Nacional de Certificadores Registrados de Costa Rica, y es un complemento del documento "Política de Certificados para la jerarquía nacional de certificadores registrados" (en adelante CP).

La Autoridad de Registro (RA) es la entidad que representa el punto de contacto entre el usuario y la Autoridad Certificadora (es la responsable por la comunicación entre el usuario y la autoridad certificadora) (en adelante CA). Está vinculada a una CA registrada y tiene por objetivo recibir, validar, verificar y gestionar las solicitudes de emisión y/o revocación de los certificados digitales, cumpliendo con lo establecido en la CP y en concordancia con otras políticas y procedimientos definidos por la CA correspondiente.

Para el presente documento se aplican las definiciones establecidas en el Decreto Ejecutivo N° 33018-MICITT "Reglamento a la Ley de certificados, firma digitales y documentos electrónicos" y sus reformas, así como el documento de la CP. Sin embargo, para ampliar la regulación de la RA se deben aclarar los siguientes conceptos:

a. Agente de registro: Persona física, responsable de la ejecución de las actividades propias de la RA. Esta persona debe estar capacitada para ejecutar sus funciones y debe realizar todas las validaciones y verificaciones definidas en la CP.

b. Confirmar la identidad del solicitante: proceso para comprobar que el solicitante es la persona con autoridad legal para solicitar el certificado digital, de acuerdo a la política asociada al certificado respectivo.

c. Suspensión de un agente de registro: Proceso mediante el cual una persona que tiene el rol de agente de registro deja de ejercer sus labores de manera temporal, denegándose sus permisos dentro del sistema de la CA.

d. Desvincular a un Agente de Registro: Proceso mediante el cual se separa de manera definitiva a un agente de registro de sus funciones, eliminándole todos los permisos dentro del sistema de la CA. Este proceso ocurre cuando:

    1. El funcionario ha renunciado a su cargo en la organización que está registrada para operar como RA.

    2. El funcionario es cesado de sus funciones o de la organización que está registrada para operar como RA.

    3. El funcionario que ha sido investido como agente de registro deja de ejercer esa función, aunque continúa trabajando en otros puestos dentro de la organización.

4. El funcionario es sancionado mediante un proceso administrativo disciplinario, que le impide continuar en su cargo.

e. Encargado de la RA: Persona física responsable de la supervisión de las funciones de los agentes de registro, y la coordinación con la CA.

f. 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 emisión y/o revocación de un certificado digital.

g. Validación del solicitante del certificado: Es el proceso mediante el cual el Agente de Registro verifica la identidad del individuo o la organización que se presente ante una RA para solicitar un certificado digital. 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.

Los procesos 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.
- Controlar y supervisar a los agentes de registro.
- La RA debe establecer los procedimientos para asegurar el cumplimiento de la CP, de este documento y de las disposiciones de la CA, además de tomar las acciones que prevengan alguna deficiencia de la RA, incluyendo la terminación o suspensión de sus deberes.

Adicionalmente, la CA es responsable de implementar procesos que permitan:

- Registrar todos los eventos de la RA en bitácoras.
- Gestionar cualquier incidente que se presente en una RA.

1.1 Administración del documento

1.1.1 Organización que administra el documento

Dirección de Gobernanza Digital

Ministerio de Ciencia, Tecnología y Telecomunicaciones, San José, Costa Rica. Sitio web: www.micitt.go.cr

1.1.2 Persona de contacto

Director de la Dirección de Gobernanza Digital, correo electrónico: firmadigital@micit.go.cr

2. Controles del Personal

2.1 Disposiciones generales

La Autoridad de Registro es la responsable administrativa de su operación y será responsable de gestionar la información actualizada de los agentes de registros activos, sus perfiles, cualidades y necesidades de acceso a la información. Esta información será debidamente custodiada según lo establece la sección 5.5.3 “Protección de Archivos” de la CP, y podrá ser solicitada en cualquier momento por la CA o la DGD como parte de sus procesos de supervisión.

Los agentes de registro pueden ser funcionarios de la organización que opera como Autoridad de Registro o en su defecto la organización puede subcontratar los servicios de una persona jurídica para este fin, en cuyo caso dicha contratación se realizará por cuenta y riesgo de la RA, entendiéndose que la RA asume la responsabilidad total sobre su gestión.

La CA deberá ser notificada sobre cualquier contratación que realice la RA con un tercero para la operación del servicio de emisión de certificados digitales. Toda la documentación de respaldo sobre contrataciones a terceros deberá constar en el expediente administrativo que al efecto lleve la CA.

2.2 Requerimientos de documentación del agente de registro

Para cada agente de registro, y en concordancia con los requisitos de personal ejecutando roles de confianza que se establecen en la sección 5.3 de la CP, la RA correspondiente deberá gestionar un expediente que cuente al menos con:

a. Un contrato de trabajo o documento que permita comprobar su situación laboral y su relación con la RA o con las empresas subcontratadas para ofrecer sus servicios.

b. Comprobante de que no tiene 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 aprobación de las capacitaciones recibidas referentes a las actividades propias de un agente de registro.

f. Declaración jurada donde afirma conocer la responsabilidad que asume al ejecutar el rol de agente de registro y el deber de cumplir con la CP, y de mantener confidencialidad y privacidad de los datos disponibles en la CA y en la RA.

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 el personal involucrado en la administración de la RA debe recibir capacitación en los siguientes temas:

a. Conceptos básicos de certificados digitales, tokens y smart cards.

b. Procedimientos operativos y de seguridad de la RA.

c. Uso del Sistema de Certificación de la CA.

d. Procedimientos para la validación y verificación de identidad.

La CA garantizará que todo agente de registro se encuentre debidamente capacitado. Las capacitaciones deberán ofrecerse nuevamente en caso de que se realicen cambios significativos en la forma en que opera la RA

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 RA deben cumplir con las siguientes exigencias mínimas de seguridad:

a. Procedimientos y/o mecanismos para la detección y atención de incendios.

b. Los equipos de la RA deben estar protegidos contra fallas del fluido eléctrico y otras anomalías en la energía.

c. Vigilancia y monitoreo del ambiente de la RA durante su horario de operación.

d. Un perímetro de seguridad en el sitio donde se ejecutan las labores de la RA, con un guarda asignado al sitio durante su horario de operación.

e. Procedimientos para evitar coacción contra cualquier agente de registro.

f. 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 (Hardening[1])

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.

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.

[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.

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 las 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 por la CA de acuerdo a los requisitos de seguridad definidos en la sección "5.5 Archivado de registros" de la CP, garantizando la confidencialidad de los mismos.

6.2 Manifiesto para la Operación de la RA

El "Manifiesto para la Operación de la RA" es una declaración jurada emitida por el responsable de la RA y custodiada por la CA, donde la RA indica que su organización cuenta con los siguientes procedimientos relacionados con la gestión de la RA:

a. Procedimientos para garantizar de continuidad del negocio.

b. Procedimientos para la gestión de los riesgos.

c. Procedimientos para sancionar faltas incurrida por los agentes de registro.

d. Procedimientos para la terminación de una RA.

e. Procedimientos para gestionar el inventario de activos de la RA.

6.3 Procedimientos de almacenamiento, manipulación y destrucción de documentos

Los documentos que componen los expedientes de los solicitantes de certificados digitales deben ser almacenados obligatoriamente en repositorios donde solo tendrán acceso los agentes de registro o los encargados de la CA.

Todos los documentos que contengan información confidencial o privada deben ser almacenados en repositorios seguros de uso exclusivo de la RA y la CA, y deberán ser destruidos sin posibilidad de recuperación cuando dejen de utilizarse.

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 CP.

8. Acuerdos operacionales

La CA debe garantizar que existe un compromiso legal por parte de la RA de acatar todo lo estipulado en la normativa vigente. En este instrumento legal también se establece quien es el responsable de la organización que gestiona la RA y que podrá ser contactado en caso de que la CA o la DGD identifiquen algún incumplimiento.