Diseño de un esquema de certificación para las Autoridades Certificadoras del Sistema Nacional de Certificación Digital de Costa Rica

Rodrigo A. Bartels[1] and Ricardo Villalón-Fonseca[2]

[1] CITIC, Universidad de Costa Rica, Costa Rica,
rodrigo.bartels@ecci.ucr.ac.cr
[2] CITIC, Universidad de Costa Rica, Costa Rica,
ricardo.villalon@ecci.ucr.ac.cr

Resumen En una Infraestructura de Llave Pública participan diversos actores, cada uno con roles diferentes dentro del proceso para emitir y usar certificados digitales, por ejemplo los usuarios, las Autoridades de Registro y las Autoridades Certificadoras (CA por sus siglas en inglés). Una CA es una entidad de confianza, responsable de emitir y revocar los certificados digitales utilizados para firmar documentos digitalmente, mitigar riesgos relacionados con el no repudio de las acciones realizadas por parte del poseedor de un certificado digital o autenticar de forma inequívoca a un ciudadano durante una transacción digital.
Este artículo presenta los resultados obtenidos al desarrollar un esquema de certificación para las Autoridades Certificadoras del Sistema Nacional de Certificación Digital de Costa Rica. El esquema desarrollado se basa en los estándares ISO 17065 y 17067, utilizados a nivel mundial para el desarrollo de sistemas de certificación y aseguramiento de la calidad en productos, procesos y servicios, y permite establecer una metodología de auditoría formal bajo el Sistema Nacional de Calidad de Costa Rica, que toma en cuenta los requisitos específicos de Costa Rica así como los estándares internacionales relevantes.

Keywords: PKI, firma digital, autoridades certificadoras, certificación

1. Introducción

Una Infraestructura de Llave Pública (PKI por sus siglas en inglés) es un sistema que utiliza certificados digitales emitidos por una entidad de confianza que se encarga de validar y asegurar la identidad y validez de los certificados emitidos [8]. Uno de los principales usos de los certificados digitales generados dentro de una PKI es la generación de firmas digitales [6].

En Costa Rica, el marco normativo para la utilización de firmas digitales se creó en 2005 con la aprobación de la Ley 8454 [3], Ley de Certificados, Firmas Digitales y Documentos Electrónicos. Esta ley define el marco legal para el uso de certificados y firmas digitales como un mecanismo equivalente a la firma manuscrita, así como su validez y aplicabilidad a documentos electrónicos, lo que

da origen al Sistema Nacional de Certificación Digital (SNCD) de Costa Rica. El SNCD es una Infraestructura de Llave Pública utilizada a nivel nacional para la generación de certificados digitales para los ciudadanos. Este certificado les permite identificarse y firmar documentos electrónicamente de forma inequívoca y no repudiable, de una forma legalmente válida y vinculante.

En abril del 2014, con el anuncio de la directriz gubernamental 067-MICITT-H-MEIC [4], el Poder Ejecutivo de la República de Costa Rica facultó al ciudadano costarricense a exigir la prestación de servicios por medio de la firma digital en todas las entidades de Gobierno. La publicación de esta directriz tuvo como principal objetivo el incrementar la transparencia en el sector público empoderando al ciudadano a tener acceso a información de carácter público mediante medios electrónicos y gratuitos y facilitar al ciudadano la utilización de los servicios públicos [5].

Paralelamente, los diversos actores involucrados en la implementación de la firma digital en Costa Rica iniciaron un proceso de auto evaluación, con el objetivo de mejorar y preparar la Infraestructura de Firma Digital para un esperado uso masivo a nivel nacional. Uno de los proyectos realizados concluyó que no existe un estándar internacional que incluya todos los requisitos que una Autoridad Certificadora tiene que cumplir en Costa Rica para poder emitir certificados digitales legalmente válidos [1]. A partir de este punto se inició un proceso de investigación con el fin de analizar el mejor mecanismo para realizar los procesos de auditoría de las Autoridades Certificadoras, requisito necesario para poder operar, y que incluya tanto los requisitos específicos de Costa Rica como los estándares internacionales relevantes (ISO-21188 [11] y Webtrust [2]).

Este artículo presenta los resultados obtenidos al desarrollar un esquema de certificación basado en estándares internacionales para el aseguramiento de la calidad de productos, procesos y servicios. Estos estándares, el *ISO/IEC 17065:2012: Evaluación de la conformidad – Requisitos para organismos que certifican productos, procesos y servicios*, y *ISO/IEC 17067:2012: Evaluación de la conformidad — Requisitos para organismos que certifican productos, procesos y servicios*, desarrollados por la Organización de Estándares Internacionales (ISO) proveen los mecanismos necesarios para el desarrollo de un sistema de certificación auto-administrado y utilizable tanto en productos tangibles y servicios.

El documento se organiza como sigue. Inicialmente se presentan un breve marco teórico con los conceptos necesarios para entender el resto del documento. Luego se describe el problema que se busca resolver, los objetivos y la metodología implementada para cumplirlos. Posteriormente se presentan los resultados obtenidos. Primero se presentan los estándares elegidos y luego se describe el esquema de certificación desarrollado. Por último se describen las conclusiones obtenidas, se menciona el impacto de la investigación y se sugieren algunos elementos como trabajo futuro.

2. Marco Teórico

Una Infraestructura de Llave Pública es un sistema que utiliza certificados digitales emitidos por una entidad de confianza, que se encarga de validar y asegurar la identidad y validez de los certificados emitidos [8]. Es difícil construir un único componente que pueda crear y distribuir de manera segura certificados digitales. Las infraestructuras de llave pública están constituidas por una variedad de componentes, cada uno de los cuales está diseñado para llevar a cabo un conjunto pequeño de tareas [6].

La Autoridad Certificadora es el componente fundamental de una Infraestructura de Llave Pública. La CA es una colección de hardware, software, procesos, regulaciones y el recurso humano que la opera. La CA es conocida por dos atributos, su nombre y su llave pública. La CA lleva a cabo tres funciones principales [8]:

1. Emite certificados: crea los certificados de los subscriptores y los firma.
2. Mantiene la información del estado de los certificados y permite la validación del estado de los certificados emitidos.
3. Mantiene archivos de la información de los estados de los certificados, ya sea expirados o revocados, que emitió.

En general las Infraestructuras de Llave Pública son utilizadas en diversos dominios de aplicación para implementar distintos casos de uso, como certificados para sitios web, firmas digitales, certificados de persona física, firma de código para aplicaciones de software, entre otros. El éxito y el correcto funcionamiento de una infraestructura de PKI depende del nivel de confianza que tengan todos los actores entre sí, y en particular hacia la Autoridad Certificadora y sus prácticas de certificación. La CA es el tercero de confianza, es el actor que sostiene la confiabilidad completa del sistema. Por esta razón, desde los inicios de la utilización de Infraestructuras de Llave Pública para la emisión de certificados para uso público, se han desarrollado guías, estándares y prácticas de aseguramiento para la evaluación de las prácticas, procedimientos y procesos de la Autoridad Certificadora, los cuales poco a poco han sido estandarizados y convertidos en normas y estándares internacionales aceptados por la industria [12]. Estos estándares son los que se utilizan como punto de partida para la evaluación y auditoría de Autoridades Certificadoras utilizadas para la emisión de certificados digitales en diversos ámbitos, por ejemplo entidades financieras, organizaciones, empresas y la implementación de infraestructuras de llave pública a nivel nacional como mecanismo de firma digital con validez legal.

En [1] se mostró que los principales estándares para la auditoría y certificación de Autoridades Certificadoras son:

1. ISO 21188:2006 Public key infrastructure for financial services – Practices and policy framework. [11]
2. Trust Service Principles and Criteria for Certification Authorities Version 2.0 – Webtrust [2]

Cuadro 1. Estándares requeridos en los países de América Latina para la implementación de Autoridades Certificadoras. Elaboración Propia.

País Estándar	Estándar Requerido
Argentina	Requisitos propios
Bolivia	Sin requisitos documentados
Brasil	Estándar Propio
Canadá	Webtrust
Chile	ETSI TS 102
Colombia	Sin requisitos documentados
Costa Rica	ISO-21188
Ecuador	ETSI TS 102
El Salvador	Sin requisitos documentados
Estados Unidos	FCPCA / Webtrust / ETSI
Guatemala	ISO-27001 / Webtrust
Haití	Sin requisitos documentados
Honduras	Requisitos propios
Jamaica	Sin requisitos documentados
México	ETSI TS 102
Nicaragua	Sin requisitos documentados
Panamá	Por definir
Paraguay	Sin requisitos documentados
Perú	ETSI TS 102
República Dominicana	Sin requisitos documentados
Unión Europea	ETSI EN 319 411 / ETSI TS 102
Uruguay	Webtrust
Venezuela	ETSI TS 102

3. ETSI TS 102 042 V2.3.1: Electronic Signatures and Infrastructures (ESI): Policy requirements for certification authorities issuing public key certificates [7]

En el mismo trabajo, se hizo un análisis de los estándares utilizados en varios países de América Latina. Estos resultados, presentados en el cuadro 1, muestran que la mayoría de los países mantienen la autonomía con respecto a la revisión de las capacidades de las autoridades certificadoras de su jerarquía. Las razones para esto sería interesante estudiarlas más a fondo en el futuro, ya que se puede conjeturar que puede ser por cuestiones económicas, desconocimiento o madurez del proceso de implementación de la Infraestructura de Llave Pública o por requisitos especiales que se requiera de las CA registradas. En todo caso, es relevante analizar que cada uno de estos países, e incluso aquellos que utilizan un estándar, necesitan un metodología para la auditoría de sus Autoridades Certificadoras.

3. Motivación y Problema

Aunque actualmente existe sólo una CA en Costa Rica (CA-SINPE) del Banco Central de Costa Rica, la ley permite la existencia de múltiples autoridades

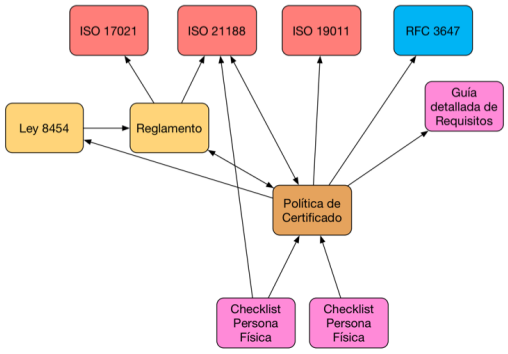

Figura 1. Documentos que contienen requisitos que una CA debe cumplir en Costa Rica y sus referencias

certificadoras, tanto públicas como privadas que deben coexistir siguiendo la reglamentación, políticas, políticas de certificado y demás requisitos establecidos por la DCFD.

En [1] se realizó un análisis de los requisitos necesarios para implementar una Autoridad Certificadora en Costa Rica y verificar si existe algún estándar internacional que los incluya. En ese trabajo se concluye que:

1. No existe un estándar internacional para certificar Autoridades Certificadoras de Infraestructuras de Llave Pública que contenga todos los objetivos de control y requisitos que se solicitan en Costa Rica.
2. En Costa Rica se pueden aplicar los estándares *ISO 21188:2006 Public key infrastructure for financial services – Practices and policy framework:* y *Trust Service Principles and Criteria for Certification Authorities Version 2.0 – Webtrust* para verificar el cumplimiento parcial de los requisitos que legalmente ocupa una CA en Costa Rica.

La Figura 1 muestra los documentos que contienen los requisitos que una Autoridad Certificadora debe cumplir y la relación de referencias entre ellos mismos. Con los documentos identificados, se revisó cada uno de ellos con el fin de extraer los requisitos que contienen. Los resultados obtenidos se muestran en el cuadro 2. En total se identificaron 593 requisitos, la mayoría de los cuales pertenecen a la Política de Certificados o al ISO-21188.

A partir de los elementos anteriores, el problema que se busca resolver es definir una metodología formal para la realización de un proceso de auditoría que permita la revisión de los requisitos especificados en los estándares internacionales pertinentes y los requisitos propios de Costa Rica.

4. Objetivos y Metodología

El objetivo principal de la investigación fue definir una metodología formal para la realización de un proceso de auditoría, que permita la revisión de los

Cuadro 2. Distribución de los requisitos de una CA por documento. Nótese que solo el ISO-21188 es un estándar internacional. Elaboración Propia.

Documento	Cantidad de Requisitos
Ley 8454	1
Reglamento a la Ley 8454	10
Política de Certificados	209
ISO-21188	340
Requisitos Técnicos-CA-PF	33
Total	593

requisitos especificados en los estándares internacionales pertinentes y los requisitos propios de Costa Rica. Para esto se siguió la metodología que se presenta en la Figura 2:

1. Revisar la literatura y consultar con expertos para identificar estándares internacionales relevantes para el aseguramiento de la calidad.
2. Seleccionar el estándar que mejor se adapte al contexto y objetivo que se busca.
3. Desarrollar una metodología de auditoría con base en el estándar seleccionado.

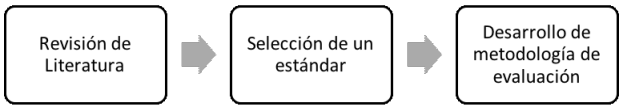

Figura 2. Metodología utilizada para la investigación.

Se presentan a continuación los resultados obtenidos.

5. Estándares para el aseguramiento de la calidad

Inicialmente se hizo una revisión de la literatura, buscando en artículos y libros, material relevante que estuviera relacionada en primera instancia con procesos de certificación y autoridades certificadoras. Los únicos estándares encontrados fueron los ya mencionados anteriormente. Luego se flexibilizó la búsqueda, y se buscaron metodologías para hacer auditoría de elementos en computación que permitieran tres características necesarias:

1. Flexibilidad en la definición de los requisitos por auditar.
2. Posibilidad de definir los requisitos de los organismos de certificación.
3. Que la metodología pudiera ser adaptada a la realidad nacional.

Cuando la búsqueda de la literatura falló, se busca ayuda de expertos en temas de aseguramiento de la calidad. Para esto, se realizaron sesiones de trabajo con expertos del Ente Costarricense de Acreditación (ECA), organismo costarricense público encargado de todos los procesos de acreditación en el país, y representante de Costa Rica ante los organismos internacionales de acreditación más importantes.

La recomendación del personal del ECA fue utilizar una nueva familia de estándares de la ISO:

1. International Organization for Standardization (ISO): ISO/IEC 17065:2012: Evaluación de la conformidad – Requisitos para organismos que certifican productos, procesos y servicios [10].
2. ISO/IEC 17067:2012: Evaluación de la conformidad — Fundamentos de la certificación de producto y directrices para los esquemas de certificación de producto [9].

Estos estándares proveen un marco para la creación de procesos de certificación definidos para:

1. Certificar productos, procesos y servicios.
2. Permite la creación de un esquema de certificación que contiene todos los elementos relevantes del proceso de certificación.
3. El dueño del esquema tiene total control sobre la estructura, el alcance, los actores y requisitos definidos en el esquema.

Con base en esta recomendación, se hizo una revisión de los estándares y se llegó a la conclusión que era factible utilizarlos y que cumplían con todos los requisitos mencionados anteriormente.

El ISO-17067 brinda los lineamientos para la creación de esquemas de certificación que son auto administrados. Este estándar se utiliza,por ejemplo, para definir esquemas de certificación de seguridad, de alimentos, de calidad de productos o servicios, entre otros. La característica principal es que la administración del estándar, así como de la definición de requisitos necesarios para obtener su certificación es competencia únicamente del dueño del estándar. Esto permite la definición de esquemas de certificación que pueden ser modificados cuando sea necesario por el ente administrador del esquema, al contrario de lo que pasa por ejemplo cuando se necesita modificar un estándar internacional como el ISO-21188 o los estándares europeos de la ETSI, en los cuales cualquier modificación necesita ser aprobada por los miembros del organismo, mediante un procedimiento largo y complejo.

El ISO-17067 brinda toda la infraestructura para la definición de un esquema de certificación diseñado a la medida de los requisitos necesarios, incluyendo referencias a estándares internacionales que se consideren necesarios. Además permite el diseño de sistemas de esquemas de certificación, en los cuáles es posible definir jerarquías de esquemas, en los cuáles los requisitos comunes a diversas situaciones pueden ser abstraídas en esquemas superiores y permitir la certificación de distintos escenarios. En este caso, se podrían desarrollar esquemas para

certificar la CA Raíz, CA Políticas y CA emisores, definiendo los requisitos comunes (la gran mayoría) en un esquema superior. El ISO-17065 por su lado, especifica todos los requisitos que deben cumplir los organismos de certificación para acreditarse y emitir certificaciones con base en el esquema desarrollado.

6. Esquema de Certificación

Para resolver el problema planteado, el hecho de que en Costa Rica, un proceso de auditoría de las Autoridades Certificadoras debe incluir elementos adicionales a los especificados en los estándares internacionales relevantes, se desarrolló un esquema de certificación con base en los estándares de la International Organization for Standardization (ISO): ISO/IEC 17065:2012: Evaluación de la conformidad – Requisitos para organismos que certifican productos, procesos y servicios, y ISO/IEC 17067:2012: Evaluación de la conformidad — Fundamentos de la certificación de producto y directrices para los esquemas de certificación de producto.

El documento desarrollado define un Esquema de Certificación para la evaluación de las Autoridades Certificadoras registradas ante la Dirección de Certificadores de Firma Digital para el Sistema Nacional de Certificación Digital. Además, a partir de este esquema se creó el Sistema de Certificación del SNCD, desarrollado con el objetivo de estandarizar los mecanismos de evaluación y certificación de los actores del SCND.

El esquema define los requerimientos para el correcto funcionamiento del proceso de auditoría y certificación, incluyendo los requisitos estructurales, legales, de recurso humano, financieros y otros que deben cumplir todos los actores involucrados en este esquema específico. Este esquema involucra directamente 3 actores:

1. Dirección de Certificadores de Firma Digital
2. Organismos certificadores acreditados
3. Autoridades Certificadoras del Sistema Nacional de Certificación Digital

La Dirección de Certificadores de Firma Digital, como ente encargado por ley de la administración y regulación del Sistema Nacional de Certificación Digital, es el dueño de este esquema de certificación y el ente encargado de la administración del esquema. Los organismos certificadores son entes legalmente acreditados bajo los requerimientos del Sistema Nacional de Calidad y el Ente Costarricense de Acreditación (ECA) para realizar auditorías y evaluaciones de las Autoridades Certificadoras del Sistema Nacional de Certificación Digital con base en los requerimientos especificados en este esquema. Las Autoridades Certificadoras son las entidades registradas para emitir certificados digitales válidos dentro del Sistema Nacional de Certificación Digital y que son emitidos para usuarios finales, ya sean personas físicas o personas jurídicas.

Cabe destacar que bajo el modelo desarrollado el peso del proceso de auditoría recae en dos de los tres actores, los organismos de certificación, como entes acreditados para certificar el esquema, y las Autoridades Certificadoras,

como entes evaluados y que buscan la certificación con base en el esquema. El rol de la Dirección de Certificadores de Firma Digital es el de supervisión y administración del esquema, con la subsecuente disminución de la complejidad y los recursos necesarios a nivel público para velar por el buen funcionamiento del Sistema Nacional de Certificación Digital. Se presentan a continuación los principales elementos que se definieron en el esquema desarrollado para cada uno de los actores principales.

6.1. Organismos Certificadores

Los organismos certificadores son organizaciones acreditadas por un ente acreditador reconocido dentro del Sistema Nacional de Calidad de Costa Rica para realizar procesos de auditoría y certificar que las Autoridades Certificadoras del SNCD cumplan con los requisitos estipulados por este esquema. El esquema agrupa los requisitos en las siguientes categorías:

- Requerimientos Legales
- Requerimientos Financieros
- Requerimientos Estructurales
- Registro y Acreditación
- Personal
- Manejo de la Imparcialidad
- Información Disponible Públicamente
- Confidencialidad
- Responsabilidad Legal

Dentro de los requisitos de registro y acreditación, se destacan dos elementos relevantes, que son los que le dan solidez al sistema de certificación, permitiendo la acreditación solamente de aquellos organismos que el dueño del esquema, en este caso la Dirección de Certificación de Firma Digital de Costa Rica, considere aptos para realizar procesos de auditoría. Estos elementos son:

1. Todo organismo certificador debe estar registrado ante la DCFD y contar con la aprobación de este ente para poder iniciar operaciones y emitir certificaciones válidas.
2. Todo organismo certificador debe obtener una certificación emitida por el Ente Costarricense de Acreditación en donde se indica que el organismo ha cumplido con todos los requisitos y ha sido acreditado para la certificación de este esquema de certificación bajo los requisitos estipulados en el estándar internacional ISO-17065.

Con base en los requisitos anteriores, el objetivo es que solamente los organismos capacitados para realizar el proceso de auditoría pueden realizar procesos de certificación con las Autoridades Certificadoras a nivel nacional.

6.2. Autoridades Certificadoras

Toda Autoridad Certificadora registrada debe tener una certificación extendida por un organismo certificador registrado ante la DCFD, con base en los requisitos especificados anteriormente. La certificación tendrá una duración de 2 años, a partir de los cuáles la Autoridad Certificadora contará con un plazo máximo de 6 meses para obtener la recertificación.

El esquema propuesto define los requisitos agrupados en las siguientes categorías:

- Requisitos
- Procedimientos de determinación del esquema
- Responsabilidad Legal

En el primer punto, el de los requisitos, el dueño del esquema define los elementos que son necesarios para obtener la certificación. En el caso de Costa Rica estos son:

1. Ser una entidad legalmente registrada ante el Registro Público.
2. Demostrar suficiente capital financiero para iniciar operaciones sin depender de los fondos obtenidos por la emisión de certificados.
3. No tener conflicto de intereses con las otras Autoridades Certificadoras registradas.
4. Contar con un representante legal, residente en Costa Rica que administre la operación de la Autoridad Certificadora.
5. Contar con una certificación con más de 6 meses de emitida que certifique que la Autoridad Certificadora cumple con todos los requisitos estipulados en el estándar Trust Service Principles and Criteria for Certification Authorities Version 2.0 (Webtrust). Esta certificación deberá ser emitida por un organismo de acreditación legalmente válida bajo los parámetros del Sistema Nacional de Calidad y el Ente Costarricense de Acreditación.

Bajo el esquema desarrollado, una Autoridad Certificadora y un Organismo Certificador deben iniciar un proceso de auditoría que siga un ciclo de certificación totalmente definido en el esquema desarrollado. Se presentan a continuación los detalles más relevantes del ciclo de certificación definido.

7. Ciclo de Certificación

El ciclo de certificación se divide en las siguientes etapas:

- Aplicación
- Aspectos Legales y Contractuales
- Proceso de Auditoría
- No conformidades
- Reporte de Evaluación
- Decisión

- Documentación de la Certificación
- Quejas y Apelaciones
- Suspensiones
- Revocaciones

Se presenta a continuación un resumen de los elementos principales dentro del proceso de certificación.

7.1. Proceso de Auditoría

El proceso de auditoría será realizado por el organismo certificador con base en los requisitos especificados en este esquema y siguiendo los lineamientos del estándar ISO-17065. En todo momento el proceso de auditoría tiene que tener un responsable encargado del proceso. Este responsable debe ser un funcionario contratado por el organismo certificador directamente y no puede ser un tercero subcontratado. El proceso de auditoría no se puede subcontratar o delegar a terceros, ya sea personas físicas o jurídicas. Si se permite la subcontratación de técnicos y expertos en auditoría para que acompañen al responsable del proceso de auditoría durante la realización de este. El proceso de auditoría se dividirá en las siguientes etapas:

1. Planeamiento: en esta etapa se discutirá la metodología de evaluación con el ente evaluado, se realizará un cronograma del plan de trabajo y se definirán los recursos encargados del ente evaluado para atender las necesidades del personal evaluador.
2. Recolección de Evidencia: En esta etapa se recolectará toda la evidencia necesaria para la determinación de cumplimiento de los requisitos del esquema.
3. Análisis: Se analizará la evidencia recolectada y se realizará un análisis de los resultados obtenidos. El responsable del proyecto deberá producir una recomendación para la decisión final que deberá tomar en cuenta los resultados y retroalimentación de todos los recursos que participaron en la evaluación.
4. Determinación: El comité nombrado para la supervisión del proceso de auditoría deberá ratificar o rechazar la recomendación hecha por el grupo evaluador. En caso de ratificación se procederá con la emisión de los certificados correspondientes.

7.2. No Conformidades

Cualquier elemento que se detecta durante el proceso de evaluación que no vaya conforme a los estándares requeridos y/o este esquema deberá ser incluido en el reporte de evaluación y comunicado al ente evaluado. Las no conformidades se clasificarán de la siguiente forma:

1. Menores: son rápidamente subsanables o no presentan mayor riesgo para el SNCD o la operación de la Autoridad Certificadora
2. Importantes: requieren mayor esfuerzo o causan el mal funcionamiento de la Autoridad Certificadora.

3. Críticas: causan un riesgo crítico para seguridad y confianza en la Autoridad Certificadora y el SNCD.

Las no conformidades menores y críticas pueden resolverse durante el proceso de auditoría y ser reevaluadas durante el mismo proceso de común acuerdo con el organismo certificador. Una no conformidad crítica implica detener el proceso de auditoría hasta que no sea subsanada. El organismo certificador deberá comunicar este tipo de no conformidades a la DCFD.

7.3. Reporte de Evaluación

Todo proceso de auditoría deberá tener un reporte de evaluación que indique:

1. El tiempo, lugar y personal que realizó el proceso de auditoría.
2. La metodología utilizada para el proceso de auditoría.
3. Las no conformidades en caso de existir.
4. Un análisis de los resultados obtenidos durante la evaluación.
5. Una recomendación de la decisión.

7.4. Documentación de la Certificación

Cuando un proceso de auditoría concluya de forma exitosa y la Autoridad Certificadora haya cumplido con todos los requisitos necesarios para la obtención de la certificación, el organismo certificador extenderá una carta y un certificado, certificando lo anterior. Este certificado deberá tener el lugar y fecha de firma, describir claramente bajo cual esquema se realizó la certificación e indicar que la afirmación de la Autoridad Certificadora de su cumplimiento de los requisitos del esquema es apoyada luego de concluido el proceso de auditoría. Tanto la carta como el certificado deberán ser firmados por el Director del organismo certificador.

7.5. Quejas y Apelaciones

En cualquier parte del proceso de auditoría el ente evaluado puede presentar una queja ante el organismo certificador siguiendo el proceso estipulado por éste, el cuál deberá estar documentado y ser incluido en el contrato firmado por las partes. El organismo certificador debe, al momento de recibir formalmente la queja, decidir si el proceso de auditoría se suspende o continúa mientras se resuelva la queja y de común acuerdo con el ente evaluado. El resultado del proceso de revisión de la queja deberá ser comunicado por escrito al ente evaluado, y tanto la queja como el resultado deberán ser incorporados a la documentación del proceso de auditoría. Si ante el resultado del proceso de evaluación de la queja, las partes no se pusieran de acuerdo, el ente evaluado puede apelar una única vez ante la DCFD, cuya resolución será final y no apelable. Las modificaciones en el alcance de la auditoría generadas por procesos de apelación o queja deberán ser incorporados al contrato original y su costo será negociado entre las partes.

7.6. Suspensiones y Revocaciones

Un organismo certificador podrá suspender en cualquier momento, una o varias de las certificaciones emitidas si:

1. Existe duda razonable de conflictos de interés, corrupción, tráfico de influencias o cualquier otra actividad punible antes, durante o después del proceso de auditoría.
2. Existe duda razonable de las capacidades o controles establecidos por una Autoridad Certificadora, con base en alguna evidencia relevante.
3. Por orden de la Dirección de Certificadores de Firma Digital. En cualquier caso, la suspensión deberá notificarse por escrito tanto a la Autoridad Certificadora como a la Dirección de Certificadores de Firma Digital. Esta notificación deberá indicar claramente:
4. Las razones para la suspensión.
5. El tiempo de la suspensión.
6. Las condiciones para el levantamiento de la suspensión.

La Autoridad Certificadora podrá apelar en instancia única la resolución de suspensión ante la Dirección de Certificadores de Firma Digital. La resolución de esta es final e inapelable.

8. Divulgación

Las Autoridades Certificadoras y los organismos certificadores tienen derechos limitados de divulgación y publicidad de la información referente a los procesos de certificación y auditoría. En caso de duda, siempre se deberá consultar con la DCFD para mitigar riesgos.

8.1. Directorio de Productos Certificados

La DCFD deberá contar con una lista pública, accesible de forma digital, de Autoridades Certificadoras registradas en el caso de la DCFD, indicando cuál organismo certificador extendió la certificación y de todos los organismos certificadores registrados. Cada organismo certificador deberá listar las Autoridades Certificadoras a las cuáles les ha extendido la certificación de este esquema.

8.2. El uso de licencias, certificados y marcas de conformidad estará regulado por la DCFD

Con el fin de incentivar el proceso de certificación y generar conciencia en las organizaciones y la ciudadanía sobre la relevancia de los procesos de auditoría y aseguramiento se desarrollo un sistema de certificados y marcas de conformidad que permite a los organismos certificados desplegar en su sitio web, publicaciones, folletos y oficinas un sello especial diseñado por la Dirección de Certificadores de Firma Digital que identifica a aquellos organismos que tienen la certificación

necesaria. Es necesario destacar aquí que la mayoría de las transacciones de firma digital en Costa Rica están relacionadas con transacciones financieras o notariales, por lo que es relevante transmitir a un usuario lo más posible una sensación de confianza y seguridad a la hora de utilizar su certificado digital.

9. Administración del Esquema

Uno de los puntos más importantes a la hora de definir el esquema, fue el hecho de tomar en cuenta que en cuestiones de tecnología, los requisitos, especificaciones y componentes tecnológicos, varían de forma rápida. Por esta razón, se definió un proceso para la administración (actualización y mejora) del esquema.

El proceso de administración del esquema sigue los siguientes lineamientos estipulados:

1. La Dirección de Certificadores de Firma Digital es el dueño de este esquema y el único en capacidad de modificar o eliminar, ya sea de forma permanente o temporal, los requisitos y normas establecidos en este esquema.
2. La Dirección de Certificadores de Firma Digital deberá tener siempre disponible la última versión de este esquema en su página web o cualquier otro medio que permita un acceso fácil y eficiente del mismo.
3. Cualquier modificación a este esquema generará una nueva versión del mismo.
4. Cualquier modificación a este esquema deberá ser comunicado a todas las Autoridades Certificadoras y organismos certificadores.
5. Las modificaciones realizadas a este esquema no afectarán las certificaciones ya extendidas o en proceso, a menos que la Dirección de Certificadores de Firma Digital indique lo contrario. En este último caso, las Autoridades Certificadoras tendrán un plazo definido por la DCFD y no menor a 3 meses, para realizar las modificaciones pertinentes en sus procesos y obtener una recertificación.
6. La Dirección de Certificados de Firma Digital puede, bajo circunstancias de excepción, convalidar o eximir uno o más requisitos incluidos en este esquema, con excepción de la certificación de Webtrust. En estos casos, la Dirección deberá justificar la decisión tomada ante el Ministro de Ciencia, Tecnología y Telecomunicaciones, y siempre se tendrá en consideración el beneficio del país y la confianza en el SNCD como parámetros para la aprobación de estas excepciones.

10. Conclusiones

Este artículo presenta el desarrollo de un esquema de certificación basado en estándares internacionales (ISO-17067 y ISO-17065) con el objetivo de realizar procesos de auditoría en Autoridades Certificadoras del Sistema Nacional de Certificación Digital de Costa Rica. El esquema de certificación desarrollado

permite aprovechar todas las metodologías y procesos definidos en los estándares de aseguramiento de la calidad para productos, procesos y servicios, con el fin de crear un marco de evaluación formal para la certificación de los procesos de una Autoridad Certificadora.

El esquema permite solventar un problema que sucede frecuentemente en aquellos dominios en los cuales los estándares internacionales de certificación son desarrollados fuera de América Latina y que no se adaptan totalmente a la realidad de los países de Latinoamérica.

Con este esquema, el Gobierno de Costa Rica tiene la capacidad de formalizar todos los requisitos necesarios para operar una Autoridad Certificadora en Costa Rica, con el subsecuente mejoramiento de los procesos de auditoría y de la solidez de la Infraestructura de Firma Digital.

11. Impacto

El desarrollo de este esquema de certificación brinda una solución para el problema que tienen muchos países de América Latina en sus Sistemas de Firma Digital. Permite formalizar un proceso de auditoría, desarrollado utilizando estándares internacionales que pueden ser certificados por entidades acreditadas. Esto hace que mediante la implementación de un esquema de este tipo, empresas que usualmente hacen certificaciones en otros ámbitos (productos, ambiente, calidad) puedan ser parte de los procesos de auditoría en infraestructuras de llave pública desarrolladas a nivel país.

12. Trabajo Futuro

A partir de los resultados presentados, el siguiente paso es iniciar el proceso de consulta pública para obtener retroalimentación sobre los elementos definidos en el esquema. También, se pretende realizar otro esquema de certificación para la auditoría de aplicaciones de software que utilizan componentes que interactúan con el Sistema Nacional de Certificación Digital, como por ejemplo firma digital, verificación de firmas y autenticación de usuarios utilizando certificados digitales.

13. Agradecimientos

La realización de este trabajo de investigación no hubiera sido posible sin la colaboración de la Dirección de Certificadores de Firma Digital del Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica, y del Área de Seguridad Tecnológica del Departamento de Seguridad y Arquitectura de la División de Servicios Tecnológicos del Banco Central de Costa Rica. Además, se agradece la ayuda obtenida del Centro de Investigaciones en Tecnologías de la Información y Comunicación (CITIC), el Posgrado en Computación e Informática y la Escuela de Ciencias de la Computación e Informática, todos de la Universidad de Costa Rica. Gracias por fomentar el trabajo de investigación y el apoyo al mejoramiento de la realidad nacional mediante este tipo de proyectos de investigación.

Referencias

1. Bartels, R.A.: Análisis de estándares internacionales para la certificación de Autoridades Certificadoras y su aplicabilidad en el Sistema Nacional de Certificación Digital de Costa Rica. Master's thesis, Universidad de Costa Rica (2016)
2. Canadian Institute of Chartered Accountants (CICA), A.I.o.C.P.A.A.: Trust service principles and criteria for certification authorities. Tech. rep. (2011)
3. de la República de Costa Rica, A.L.: Ley de certificados, firmas digitales y documentos electrónicos (2005)
4. de Costa Rica, G.: Masificación de la implementación y el uso de la firma digital en el sector público costarricense (136)
5. GobiernoCR: Firma digital superó los 100 mil certificados digitales, http://gobierno.cr/firma-digital-supero-los-100-mil-certificados-digitales/
6. Housley, Russ; Polk, T.: Planning for PKI. Wiley Computer Publishing (2001)
7. Institute, E.T.S.: Electronic signatures and infrastructures (esi); policy requirements for certification authorities issuing public key certificates. Tech. Rep. ETSI TS 102 042 (2013)
8. Johannes A. Buchmann, Evangelos Karatsiolis, A.W.: Introduction to Public Key Infrastructures. Springer (2013)
9. Organization, I.S.: 17065:2013 conformity assessment – requirements for bodies certifying products, processes and services. Tech. rep., ISO/IEC (2013)
10. Organization, I.S.: 17067:2013 conformity assessment – fundamentals of product certification and guidelines for product certification schemes. Tech. rep., ISO/IEC (2013)
11. for Standardization, I.O.: Norma inte/iso 21188:2007 infraestructura de llave pública para servicios financieros - estructura de prácticas y políticas. Tech. rep., International Organization for Standardization (2007)
12. Stapleton, J., Epstein, W.C.: Security without Obscurity: A Guide to PKI Operations. Auerbach Publications (2016)