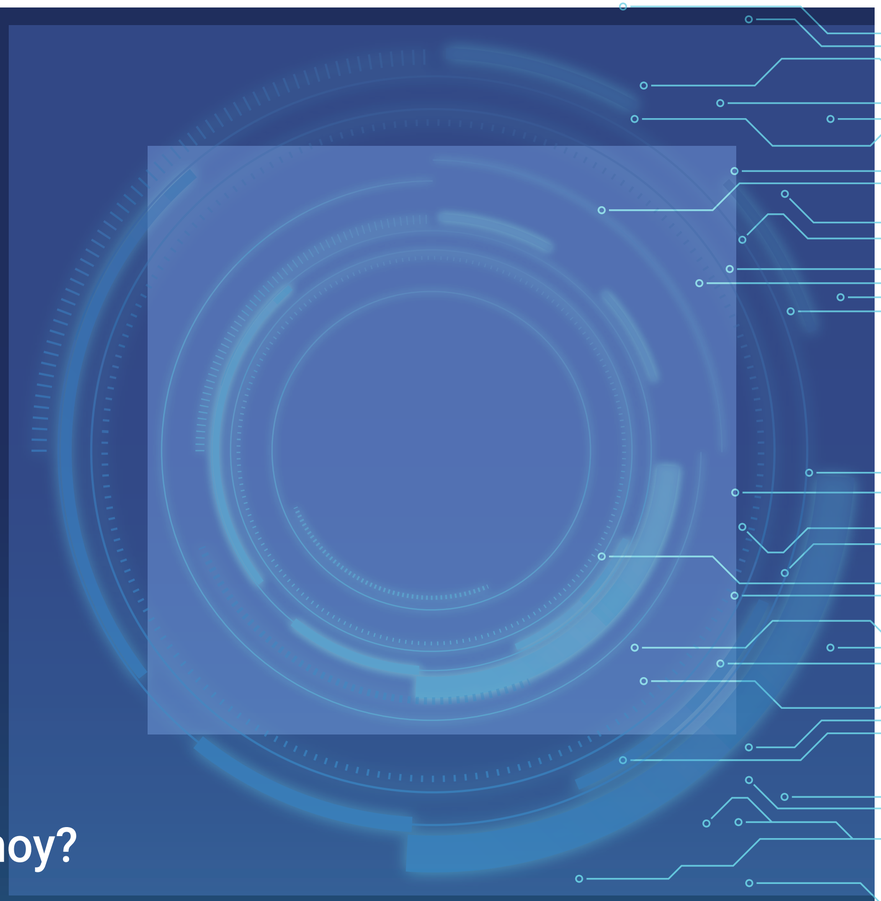
CertiSur



DISCOVERY & AUTOMATION:
Claves para una Gestión Eficiente de Certificados Digitales

Índice

1. La nueva realidad de los certificados digitales
2. Riesgos del enfoque manual o fragmentado
3. Descubrimiento continuo: ver para gestionar
4. Automatización inteligente: del caos al control
5. Integración con el ecosistema tecnológico
6. Lo que debe ofrecer una buena solución
7. Checklist de madurez: ¿Dónde está tu organización hoy?
8. Conclusión: de la visibilidad al valor
9. Glosario



INTRODUCCIÓN:

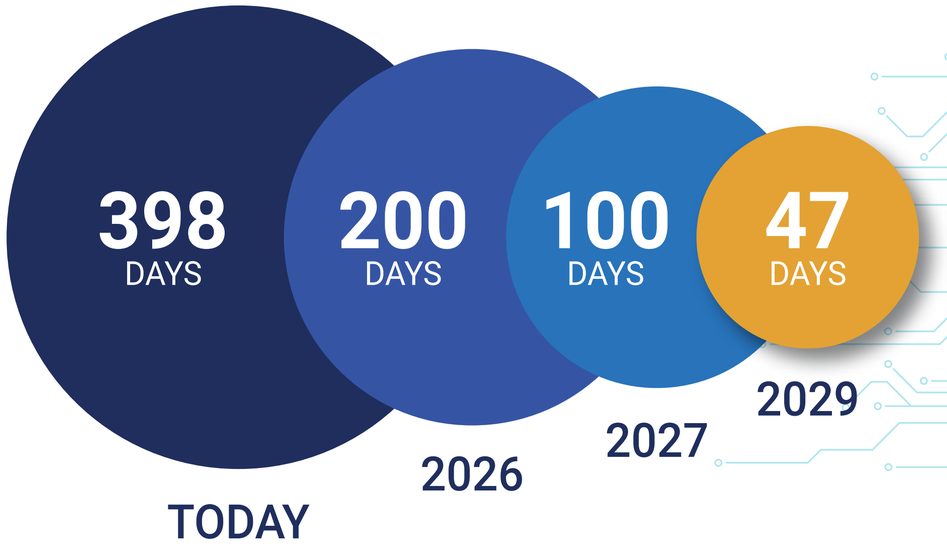
La nueva realidad de los certificados digitales

En un entorno tecnológico cada vez más distribuido y dinámico, **las identidades digitales se han vuelto el corazón de la seguridad de la información.** Desde servicios web y contenedores hasta dispositivos móviles y entornos multicloud, el volumen de certificados digitales crece de forma constante.

Cada certificado cumple funciones clave: cifrado, autenticación y confianza. Sin embargo, muchas organizaciones siguen gestionándolos de manera manual o fragmentada. **El problema no es sólo operativo, sino estratégico: cada certificado no visibilizado o no gestionado representa un riesgo latente.**

Las interrupciones por expiraciones no detectadas, las fallas en auditorías o el uso de algoritmos inseguros pueden tener un impacto directo en la reputación y continuidad del negocio. **En este contexto, la visibilidad total y la automatización del ciclo de vida de los certificados ya no son un lujo, sino una necesidad urgente.**

Además, el cambio hacia certificados con una vigencia más corta



SEGURIDAD
preparada para el futuro:

- Mitigar riesgos actuales.
- Reducir el tiempo de exposición a vulnerabilidades.
- Fortalecer la confianza.
- Preparar la infraestructura para la criptografía post-cuántica

(impulsado por navegadores como Chrome y Apple) marca el fin de la gestión manual. Con la aprobación reciente de la reducción a certificados públicos con validez de sólo 47 días, se hace evidente la necesidad urgente de adoptar una gestión moderna y automatizada.

Además, la votación SC-81v3 aprobada en el CA/Browser Forum impulsa una reducción progresiva tanto en la validez de los certificados como en la reutilización de datos verificados. Esto impactará de forma directa en los procesos manuales de emisión, reforzando la necesidad de automatización a través de protocolos como ACME.

Y por último, **con el avance de la computación cuántica, se abre un nuevo frente de preocupación: los algoritmos criptográficos tradicionales podrían volverse vulnerables en un futuro no tan lejano.**

Prepararse para un entorno post-cuántico implica conocer con precisión qué certificados existen, qué algoritmos utilizan y cómo planificar su migración. En este sentido, el descubrimiento, la visibilidad y automatización también se vuelven claves para afrontar la transición hacia una criptografía resistente a la computación cuántica (PQC).

Este eBook busca exponer esas necesidades y ofrecer una guía práctica para entender por qué Discovery & Automation es el camino para una gestión moderna, eficiente y segura de los certificados digitales.

“**LA AUTOMATIZACIÓN,**
ya no es una opción técnica:
es una decisión estratégica
para asegurar ***continuidad,***
cumplimiento y confianza digital
en un contexto que cambia día a día.”

Néstor Markowicz - *COO de CertiSur*

CAPÍTULO 2:

Riesgos del enfoque manual o fragmentado

La gestión manual de certificados digitales puede parecer viable cuando se trata de unos pocos activos. Sin embargo, **a medida que las organizaciones crecen, también lo hace el volumen de certificados distribuidos entre distintas plataformas, entornos y equipos.**

Muchas empresas siguen utilizando planillas de cálculo, recordatorios en calendarios. Estas prácticas generan silos de información, falta de visibilidad global y una alta dependencia de procesos humanos propensos al error.

Elemento	Hoy	Desde el 15/03/2026	Desde el 15/03/2027	Desde el 15/03/2029
Info verificada del sujeto (SubjectDN)	825 días	398 días	398 días	398 días
Reutilización de nombre de dominio/IP	398 días	200 días	100 días	10 días
Validez del certificado	398 días	200 días	100 días	47 días

Administrar certificados manualmente ya no es sostenible. Con una vigencia de apenas 47 días y nuevos requisitos que limitan la reutilización de datos verificados, las organizaciones se enfrentarán a un volumen de renovaciones mensuales imposible de manejar sin herramientas automatizadas.

Este escenario expone a los equipos de IT a:

- **Expiraciones no detectadas:** Un certificado olvidado puede causar la caída de un sitio web, la interrupción de servicios críticos o la pérdida de confianza por parte de los usuarios.
- **Falta de cumplimiento:** Auditorías de seguridad o normativas como PCI-DSS, ISO 27001 o regulaciones bancarias exigen control centralizado y trazabilidad sobre los certificados utilizados.
- **Vulnerabilidades latentes:** Sin una revisión sistemática, pueden persistir certificados emitidos con algoritmos obsoletos o claves comprometidas.
- **Reacción tardía ante incidentes:** En caso de una revocación masiva o compromiso de una Autoridad Certificante CA, sin inventario actualizado es imposible actuar con rapidez.

Según el **DigiCert Trust Survey**, el 45% de las empresas encuestadas reportaron haber sufrido interrupciones de servicio en el último año debido a incidentes relacionados con certificados digitales y de estos episodios, un 37,5% se atribuyen específicamente a certificados expirados, una de las causas más prevenibles de estas interrupciones.

Frente a esta realidad, se vuelve imprescindible contar con una solución que unifique la gestión, automatice tareas repetitivas y brinde visibilidad en tiempo real. La evolución hacia una plataforma de Discovery & Automation permite transformar un proceso frágil y reactivo en uno predecible y resiliente.

> Riesgos de vencimientos y caídas de servicios.
> Brechas de seguridad y daño reputacional.
> Incumplimiento normativo y sanciones económicas.
> Sobrecarga operativa y dependencia de recursos técnicos.

CAPÍTULO 3:

Descubrimiento continuo: ver para gestionar

No se puede proteger lo que no se puede ver. En este contexto el descubrimiento continuo es el primer paso para el control total. Identificar todos los certificados activos, sin importar dónde se encuentren o con qué CA fueron emitidos.

El desafío es que muchos de estos certificados son desconocidos para los equipos de seguridad, lo que incrementa significativamente el riesgo operativo.



Una solución moderna de descubrimiento debe ofrecer:

- **Cobertura integral:** Capacidad de detectar certificados públicos y privados en redes internas, externas y en múltiples entornos tecnológicos.
- **Múltiples métodos de escaneo:** Desde sincronización con bases de datos de autoridades certificantes hasta análisis en dispositivos y entornos virtuales.
- **Actualización en tiempo real:** El inventario debe mantenerse siempre al día, sin depender de escaneos manuales o esporádicos.
- **Visibilidad contextual:** Ver los detalles críticos: algoritmo, fecha de expiración, emisor, uso, y a qué servicios están vinculados.

Entonces no es una tarea puntual, sino un proceso continuo que permite actuar de forma proactiva y con datos confiables.
Una vez identificados, los certificados pueden clasificarse, agruparse y vincularse a responsables, facilitando su monitoreo.

> Una buena estrategia de descubrimiento previene certificados no monitoreados, minimiza el riesgo de interrupciones y garantiza un punto de partida sólido para la automatización.

CAPÍTULO 4:

Automatización inteligente: del caos al control

Contar con un inventario completo de certificados es un gran paso, pero no alcanza si las tareas asociadas a su ciclo de vida siguen dependiendo de la intervención manual. Aquí es donde entra en juego la automatización.

La automatización del ciclo de vida de los certificados permite gestionar de manera ágil, segura y eficiente procesos como:

- **Emisión**
- **Renovación**
- **Instalación**
- **Revocación**



Estas acciones pueden configurarse para ejecutarse automáticamente en función de políticas predefinidas, minimizando el riesgo de error humano y reduciendo drásticamente los tiempos de respuesta ante incidentes o auditorías.

Los principales beneficios incluyen:

- **Reducción de tiempos operativos:** Menos horas dedicadas a tareas repetitivas.
- **Mitigación de riesgos:** Evita vencimientos, configuraciones incorrectas o instalaciones fallidas.
- **Consistencia:** Aplicación uniforme de políticas criptográficas en toda la organización.
- **Escalabilidad:** Permite gestionar miles de certificados sin esfuerzo adicional.

En este nuevo escenario, los protocolos se vuelven fundamentales para sostener la operación y garantizar continuidad sin sobrecargar los equipos técnicos.

Una solución moderna debe incluir capacidades como generación automática de Certificate Signing Request (CSR)*1*, integración con sistemas IT Service Management (ITSM)*2*, mecanismos de aprobación por roles y workflows personalizables.

En definitiva, la automatización transforma una operación reactiva y fragmentada en un proceso predecible, gobernado por políticas claras de seguridad.

Las Plataformas modernas DEBEN PERMITIR:

> Renovación automática y planificada de certificados.

> Integración con protocolos como ACME, SCEP, EST o APIs REST. *3*

> Instalación sin intervención manual en servidores, balanceadores, contenedores y entornos cloud.

“Con ciclos de vida **más cortos** y validaciones **más frecuentes**, solo **LA AUTOMATIZACIÓN** permite escalar ***la seguridad sin comprometer la agilidad.***”

Dean Coclin
Director Senior de Desarrollo Comercial, DigiCert

CAPÍTULO 5:

Integración con el ecosistema tecnológico

Los certificados viven en una variedad de entornos, interactúan con múltiples sistemas y son utilizados por diversos equipos. Por eso, una solución de Discovery & Automation efectiva debe adaptarse al ecosistema tecnológico existente y no al revés.

Una plataforma moderna debe integrarse con:

- **Sistemas de red y servidores:** Web servers, balanceadores de carga, proxies, firewalls, dispositivos móviles y más.
- **Herramientas DevOps y CI/CD:** Entornos de desarrollo ágil necesitan emitir y renovar certificados de forma automatizada, sin fricción.
- **Sistemas ITSM y gestión de incidentes:** Para registrar solicitudes, aplicar flujos de aprobación y mantener trazabilidad.
- **Cloud y contenedores:** Los certificados deben moverse al ritmo de las cargas de trabajo dinámicas en entornos multicloud y Kubernetes.
- **Vaults, HSMs y PAMs:** Para el manejo seguro de claves privadas y credenciales, siguiendo el principio de mínimo privilegio.

Una integración real permite visibilidad completa y acciones automatizadas sin reestructurar procesos existentes. Así, Discovery & Automation se convierte en una plataforma eficiente, segura y que cumple con el ecosistema.

> La gestión de certificados ya no puede depender de soluciones aisladas.

> La interoperabilidad y la integración con el stack tecnológico existente son la clave para mantener el control sin frenar la innovación.

CAPÍTULO 6:

Lo que debe ofrecer una buena solución

A la hora de seleccionar una herramienta de gestión, es clave evitar soluciones que, aunque prometen simplicidad, imponen limitaciones o generan dependencia tecnológica.

Una solución robusta debe reunir las siguientes características:

- **Independencia de la CA:** Debe poder gestionar certificados de múltiples proveedores, públicos o privados.
- **Capacidad de gestionar lo existente:** Debe poder descubrir, inventariar y controlar certificados ya emitidos, sin necesidad de revocar y volver a emitir.
- **Arquitectura modular y escalable:** Evitar soluciones tipo middleware que interrumpan los flujos existentes. Debe poder adaptarse a distintos entornos sin imponer un rediseño completo.
- **Seguridad por diseño:** Controles de acceso granulares, gestión segura de claves privadas, integración con HSMs y trazabilidad completa de acciones.
- **Interfaz intuitiva y roles diferenciados:** Paneles de control personalizables para distintos perfiles (infraestructura, seguridad, cumplimiento, etc.) con funciones adecuadas y segmentadas.
- **Flexibilidad en la implementación:** Que pueda ser desplegada on-premise, en la nube, o como servicio, de acuerdo a las necesidades del cliente.

Además, es importante evitar:

- Bloqueos tecnológicos por parte del proveedor.
- Soluciones que sólo detectan certificados a través del tráfico de red, sin visibilidad completa.
- Plataformas que no permitan integración con los sistemas existentes.
- Herramientas con costos por certificado que limiten el alcance de la solución.

En resumen, una buena solución debe permitir evolucionar hacia una gestión proactiva, completa y alineada con los objetivos de seguridad de la organización, sin forzar cambios innecesarios ni imponer limitaciones en el camino.

“La verdadera **TRANSFORMACIÓN** ocurre cuando la gestión de certificados **se integra en el ADN operativo de la organización.** La automatización no debe ser un parche: ***debe ser parte del diseño.***”

Murali Palanisamy
Chief Solutions Officer, AppViewX

CAPÍTULO 7:

Checklist de madurez: *¿Dónde está tu organización hoy?*

Adoptar Discovery & Automation no es un salto único, sino un camino evolutivo. Muchas organizaciones se encuentran en diferentes etapas de madurez en lo que respecta a la gestión de certificados. Este checklist te permitirá identificar tu situación actual y trazar un plan claro de mejora.

VISIBILIDAD

- ¿Contamos con un inventario completo y actualizado de todos los certificados digitales?
- ¿Tenemos identificados los emisores (CAs) y los algoritmos utilizados por cada certificado?
- ¿Podemos ver desde una única consola el estado y vencimiento de cada certificado?
- ¿Contamos con alertas o reportes ante vencimientos próximos o configuraciones incorrectas?
- ¿Detectamos certificados no autorizados, auto-firmados o sin propietario asignado?

SI	NO

AUTOMATIZACIÓN

- ¿Qué porcentaje del ciclo de vida de los certificados (emisión, renovación, instalación, revocación) está automatizado?
- ¿Utilizamos protocolos de automatización como ACME, SCEP, EST o APIs REST?
- ¿Se ejecutan renovaciones de forma anticipada y controlada, sin intervención humana?
- ¿Contamos con workflows automatizados para aprobaciones o distribución en entornos críticos?

GOBERNANZA

- ¿Quiénes son responsables de cada certificado?
- ¿Tenemos segmentación de roles y permisos sobre la gestión de certificados?
- ¿Podemos generar reportes para auditorías y cumplimiento normativo?

SEGURIDAD Y CUMPLIMIENTO

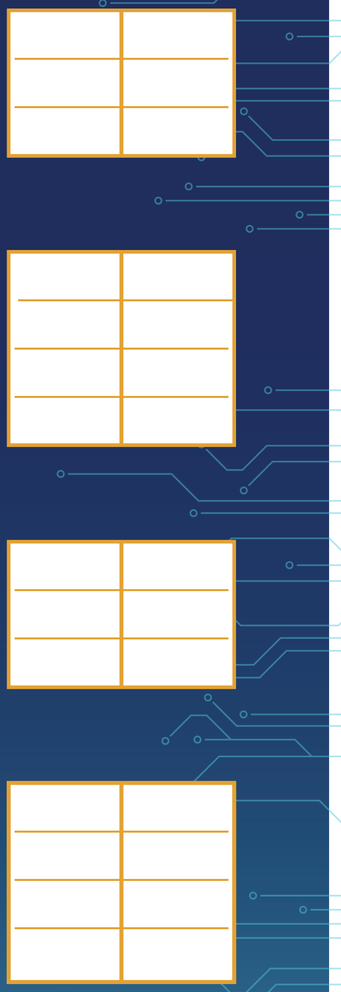
- ¿Se aplican políticas criptográficas consistentes (longitud de clave, algoritmos, validación)?
- ¿Contamos con segregación de funciones y controles de acceso por roles?
- ¿Auditamos regularmente los cambios y eventos asociados a la gestión de certificados?
- ¿Estamos preparados para responder ante compromisos de una CA o fallas masivas?

INTEGRACIÓN TECNOLÓGICA

- ¿La gestión de certificados está integrada a nuestras plataformas DevOps, ITSM, cloud y dispositivos de red?
- ¿Podemos gestionar certificados en entornos híbridos, contenedores y microservicios?
- ¿Nuestro modelo actual permite escalar sin reestructurar la infraestructura existente?

PREPARACIÓN PARA EL FUTURO

- ¿Estamos al tanto del Ballot SC-81v3 y sus implicancias sobre la reutilización de datos verificados?
- ¿Tenemos un plan para adaptarnos a certificados con vigencia de 47 días?
- ¿Estamos evaluando la migración a algoritmos post-cuánticos (PQC)?
- ¿Tenemos la capacidad de identificar rápidamente los certificados que deberán ser reemplazados ante una nueva amenaza?



CAPÍTULO 8:

Conclusión: de la visibilidad al valor

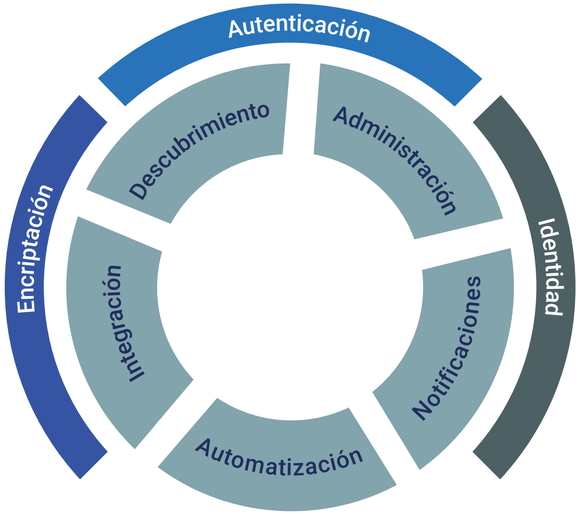
El crecimiento explosivo de certificados digitales en las organizaciones no se detendrá. Lejos de eso, se intensificará a medida que las arquitecturas se vuelvan más distribuidas, las aplicaciones más dinámicas y los requisitos de seguridad más exigentes.

En este escenario, confiar en métodos manuales o fragmentados no solo es ineficiente: es riesgoso. La falta de visibilidad, la imposibilidad de reaccionar rápidamente y la sobrecarga operativa son barreras que impiden alcanzar una postura de seguridad madura.

Discovery & Automation no es una simple herramienta técnica. Es una capacidad estratégica que permite anticiparse a problemas, optimizar recursos y alinear la gestión de certificados con los objetivos del negocio.

Una buena implementación permite:

- Evitar interrupciones imprevistas.
- Reducir costos operativos.
- Cumplir con normativas y auditorías.
- Prepararse para escenarios futuros como la computación cuántica.



> La visibilidad es el primer paso.
> La automatización es el camino.
> El valor está en el control.

Desde **CertiSur** impulsamos esta transformación porque creemos en construir entornos digitales más seguros, confiables y resilientes. Esperamos que este eBook te haya ofrecido un punto de partida claro para pensar estratégicamente la gestión de certificados digitales en tu organización.

“La gestión moderna de **certificados digitales ya no es una opción:** es una **necesidad estratégica**. **AUTOMATIZAR Y DESCUBRIR** en tiempo real no solo reduce riesgos, sino que ***fortalece la confianza digital en el corazón del negocio.***”

Néstor Markowicz - *COO de CertiSur*

Sobre CertiSur

En **CertiSur** llevamos más de 25 años acompañando a organizaciones de todo tipo en la implementación de soluciones de seguridad digital robustas, confiables y escalables. Nuestra experiencia en la gestión del ciclo de vida de certificados, autenticación e identidad digital nos posiciona como un partner estratégico para mitigar riesgos, cumplir con regulaciones y facilitar la transformación segura de los procesos de negocio.

Hoy más que nunca, **contar con una infraestructura de confianza exige visibilidad completa y automatización inteligente.**

¿Estás listo para simplificar y asegurar la gestión de tus certificados digitales?

Descubrí cómo CertiSur puede ayudarte a implementar un enfoque automatizado y centralizado, alineado con las mejores prácticas del mercado.

Solicitá una demo

sales@certisur.com

Glosario

1- Certificate Signing Request (CSR), que es el archivo que contiene la información necesaria para solicitar un certificado digital a una Autoridad Certificante (CA). Un **CSR** incluye: **el nombre de dominio** para el que se solicita el certificado, la **clave pública** que formará parte del certificado, información de la organización (nombre, ubicación, etc.) y el algoritmo de cifrado usado.

2- La **integración con sistemas ITSM (IT Service Management)** significa conectar con herramientas que usa el equipo de IT para gestionar tickets, incidentes, cambios y solicitudes.

3- Protocolo **ACME (Automated Certificate Management Environment)**: Protocolo abierto desarrollado por la Internet Security Research Group (ISRG) que permite a los sistemas solicitar, renovar e instalar certificados digitales de forma automática. Mientras que el **SCEP (Simple Certificate Enrollment Protocol)** es un protocolo diseñado para simplificar la solicitud y emisión de certificados en dispositivos de red como routers, firewalls o endpoints, que les permite generar una clave, crear un CSR y obtener un certificado de una CA de forma automatizada. Sobre **EST (Enrollment over Secure Transport)** se trata de un protocolo moderno y seguro para el enrolamiento de certificados a través de HTTPS, que añade mayor seguridad para nuevos algoritmos criptográficos.

4- CI/CD: Continuous Integration / Continuous Delivery. Automatiza la compilación, prueba y despliegue de software en entornos de prueba y producción.

Bibliografía

Bank for International Settlements – BIS has published "Quantum-readiness for the financial system: a roadmap"
https://www.bis.org/publ/bppdf/bispap158.htm

02 JUL 2025 European Commission officially launched its Quantum Strategy
https://digital-strategy.ec.europa.eu/en/library/quantum-europe-strategy

Quantum for dummies de digicert
https://www.digicert.com/campaigns/pqc-for-dummies-ebook

DigiCert Trust Pulse Survey
https://www.digicert.com/news/digicert-survey-finds-manual-processes-expose-organizations

What are the five stages of the certificate lifecycle?
https://www.digicert.com/faq/certificate-management/what-are-the-five-stages-in-the-certificate-lifecycle

AppViewX Certificate Lifecycle Management (CLM) Maturity Model
https://pages.appviewx.com/certificate-lifecycle-management-maturity-model.html

CertiSur

www.certisur.com