Universidad CENFOTEC
Maestría en Ciberseguridad

Tema:

Propuesta de mejora ágil en el sistema software gestor de certificados digitales Enterprise para Intel

Elaborado por:
Romel Espinoza Chaves

Fecha: Junio, 2024

Declaratoria de derechos de autor

El presente trabajo de tesis es un documento original, elaborado por mi persona como requisito para la obtención del título de Master en Ciberseguridad, en la universidad CENFOTEC.

Este trabajo es de mi autoría y propiedad intelectual, y no ha sido presentado previamente para ningún otro fin académico o de publicación, declaro que he respetado los derechos de autor de las fuentes consultadas para la realización de esta tesis, y que todas las citas y referencias a otros trabajos han sido debidamente identificadas y atribuidas según las normas académicas correspondientes.

Autorizo a la Universidad CENFOTEC a publicar esta tesis en su repositorio institucional, en formato digital, respetando en todo momento los derechos de autor.

Agradecimientos

Al Profesor Roy E. Valenciano González. Sin usted, sin sus recomendaciones, su paciencia, su compromiso y constancia, este trabajo no lo hubiese logrado. Sus consejos fueron siempre clave para lograr terminar este objetivo de vida (una maestría). Usted formó parte importante de esta historia con sus aportes profesionales que lo caracterizan. Siempre estaré agradecido.

A mi novia Daniela Rodriguez Valerio, por acompañarme, por escucharme, por corregirme, gracias por sus múltiples palabras de aliento cuando más las necesite, no puedo dejar de recordar cuantas tardes y horas de trabajo juntos a lo largo de este proyecto. Hoy me toca cerrar un capítulo maravilloso y no puedo dejar de agradecerte por su apoyo incondicional.

A la Universidad CENFOTEC mis más sincero agradecimiento por la oportunidad, la flexibilidad y el apoyo que me han brindado durante mi tiempo en esta maestría. Ha sido un camino largo y empinado, pero ha valido la pena el esfuerzo, la educación que he recibido en esta institución ha sido invaluable, moldeando mi conocimiento, habilidades y perspectiva de una manera que me ha preparado para un mejor futuro.

Dedicatoria

Primero deseo dedicar este TFG a Dios, ya que sin él no hubiera logrado culminar esta meta de vida, hubo múltiples obstáculos en el camino, pero Dios hizo su trabajo para que yo pudiera terminarlo.

Segundo se lo dedico a mi hijo Rodrigo Espinoza quien es mi motor de vida y mi inspiración para terminar este proyecto, quiero dejarle este recuerdo a mi hijo, un papá que siempre se esforzó por cumplir metas personales.

A mis papás que me dieron la vida, por ser unos padres ejemplares, siempre lucharon por sus hijos, me inculcaron el valor del estudio y la educación.

Tabla de contenido

Abstract 1

Capítulo 1. Introducción 2

1.1 Generalidades 2

1.2 Antecedentes del Problema 2

1.3 Definición y Descripción del Problema 3

1.4 Justificación 6

1.5 Viabilidad 7

1.5.1 Punto de Vista Técnico. 7

1.5.2 Punto de Vista Operativo. 8

1.5.3 Punto de Vista Económico. 8

1.6 Objetivos 9

1.6.1 Objetivo General 9

1.6.2 Objetivos Específicos. 9

1.7 Alcances y Limitaciones 9

1.7.1 Alcances. 9

1.7.2 Limitaciones. 10

1.8 Marco de Referencia Organizacional y Socioeconómico 10

1.8.1 Historia. 10

1.8.2 Tipo de Negocio y Mercado Meta. 12

1.8.3 Misión, Visión y Valores. 13

1.8.4 Políticas Institucionales. 13

1.9 Estado de la Cuestión 15

1.9.1 Planificación de la revisión 16

1.9.2 Ejecución de la revisión 20

1.9.3 Resumen de los resultados 44

Capítulo 2. Marco Conceptual 45

2.1 Red y comunicación de datos 46

2.1.2 Autenticación 47

2.1.3 Llave Pública / llave privada 49

2.1.4 Internet Standard X.509 49

2.1.5 Certificados de autenticación TLS/SSL 51

2.1.6 Autoridad de certificación (AC) 52

2.2 Gestión Certificados digitales 54

2.2.1 Ciclo de vida certificados digitales 57

2.2.2 Administración certificados digitales 58

2.2.3 Automatización certificados digitales 58

Capítulo 3. Marco Metodológico 60

3.1 Tipo de Investigación 60

3.2 Alcance Investigativo 61

3.2.1 Explicativo 61

3.2.2 Descriptivo: 61

3.3 Enfoque 62

3.3.1 Epistemológica..... 62

3.3.2 Ontológico..... 63

3.3.3 Axiológico..... 63

3.4 Diseño..... 66

3.5 Población y Muestreo..... 66

3.6 Instrumentos de Recolección de Datos 68

3.7 Técnicas de Análisis de Información..... 73

3.8 Estrategia de Desarrollo de la Propuesta..... 73

Capítulo 4. Análisis del Diagnóstico 74

4.1 Aplicación de entrevista a expertos 74

4.1.1 Resultados de entrevista a representante experto del equipo PEIT QUALITY& STRESS LABS..... 75

4.1.2 Resultado de entrevista a representantes expertos del equipo IT EOG EPSE Data & PLTF 76

4.1.3 Resultados de entrevista a representante experto del equipo Supply Chain Source & Procure..... 80

4.1.4 Resultado de entrevista a representantes expertos del equipo IT EOG ICC Ctrl Escalation Mgr..... 81

4.2 Análisis de resultados. 85

4.2.1 Generalidades..... 85

4.2.2 Pilares de seguridad y manejo manual de los certificados digitales. 86

Capítulo 5. Propuesta de Solución..... 90

5.1 Descubrimiento e investigación de soluciones de software para el manejo del ciclo de vida de certificados digitales enterprise disponibles en el mercado..... 91

5.2 Documentación y desarrollo de las herramientas identificadas. 91

5.2.1 Herramienta Venafi TPP 92

5.2.2 Herramienta APPVIEWX Platform 104

5.3 Comparación de las herramientas. 116

5.4 Creación manual técnico..... 118

Capítulo 6. Conclusiones y recomendaciones 126

6.1 Conclusiones 126

6.2 Recomendaciones 128

Referencias..... 130

Índice de tablas

Tabla 1*: Costo de horas consultor* 8

Tabla 2: *Listado de palabras.* 16

Tabla 3: *Publicaciones seleccionadas Google Scholar.* 21

Tabla 4: *Publicación #1* 23

Tabla 5: *Publicación #2* 26

Tabla 6: *Publicación #3* 27

Tabla 7: *Publicación #4* 30

Tabla 8: *Publicación #5* 32

Tabla 9: *Publicación #6* 33

Tabla 10: *Publicación #7* 36

Tabla 11: *Publicaciones seleccionadas researchgate.net.* 41

Tabla 12: *Publicación #8* 41

Tabla 13*: Publicación #9* 42

Tabla 14*: Análisis de resultados* 44

Tabla 15 *Criterio de evaluación* 64

Tabla 16 *Expertos entrevistados* 67

Tabla 17 *Respuestas de PE1* 75

Tabla 18 *Respuestas de PE2 y PE3* 76

Tabla 19 *Respuestas de PE4* 80

Tabla 20 *Respuestas de PE5 y PE6* 82

Tabla 21 *Venafi TPP Integraciones* 95

Tabla 22 *AppViewX Integraciones* 107

Tabla 23 *Evaluación de categorías* 117

Índice de figuras

Fig. 1 Método de selección de artículos. 20

Fig. 2 Nube de palabras utilizando herramienta nubedepalabras.es. 45

Fig. 3 Mapa conceptual Jerárquico conceptos 46

Fig. 4 Ciclo de vida certificados digitales. 57

Fig. 5 Encuesta a toda la población de dueños de aplicaciones para la compañía. 72

Fig. 6 Diagrama de espina de pescado. 73

Fig. 7 Fases para desarrollo de la propuesta 90

Fig. 8 Venafi TPP Arquitectura. 97

Fig. 9: AppViewX CERT+ Arquitectura 109

Abstract

El presente trabajo final de graduación tuvo como objetivo general proponer una mejora ágil en el sistema software gestor de certificados digitales Enterprise para la empresa transnacional Intel. Por lo tanto, se realizó un diagnóstico del panorama actual respecto al manejo del ciclo de vida de certificados digitales en la mencionada empresa, con lo cual se encontró que no hay procedimientos estándares ni automatización. Este panorama y el continuo crecimiento de certificados de servidor TLS entre distintos departamentos, distintas redes y distintos sistemas presentan un desafío único en la implementación de un programa de gestión de certificados eficaz en un entorno empresarial.

Dentro de los principales impactos negativos que resultan de una mala gestión de certificados están:

1- Interrupciones en aplicaciones importantes, causadas por certificados vencidos. Impactando la imagen de la organización
2- Riesgo en violaciones de seguridad resultantes de la suplantación de servidores.
3- Interrupciones o violaciones de seguridad resultantes de la falta de criptoagilidad.
4- Una mayor vulnerabilidad a ataques a través de amenazas cifradas.

A raíz de esta situación es que esta investigación sugiere la automatización completa de la gestión del ciclo de vida de los certificados digitales. Por lo que a través de un análisis de las herramientas disponibles en el mercado se concluyó que Venafi TPP es la plataforma que mejor se adapta a las necesidades y requerimientos de Intel.

Capítulo 1. Introducción

1.1 Generalidades

Esta investigación tiene como propósito proveer una solución permanente a una falla en el ciclo de vida de los certificados digitales, sin embargo, por razones de seguridad de la información, no se mencionan detalles técnicos de la compañía como ningún tipo de especificaciones de arquitectura de software, documentos de diseño de software de alto nivel, flujos de datos, diagramas de infraestructura de red o de plataformas, ningún tipo de código, manuales de referencia del programador, documentación de procesos internos para software, especificaciones del BIOS y pautas de ajuste, guías del escritor de BIOS, nombres de soluciones software en uso, datos como direcciones ip o nombres de servidores, firmware del producto, validaciones de software, pruebas de compatibilidad y vulnerabilidad, kits de desarrollo de software, herramientas de desarrollo de software que permiten a los clientes desarrollar, analizar o depurar sus diseños utilizando productos Intel, tecnología de arranque rápido de software, SaaS y detalles técnicos o datos de los certificados. Se solicita una cláusula de confidencialidad entre la universidad e Intel.

1.2 Antecedentes del Problema

Como medida de mitigación inmediata y de corto plazo se formó un equipo centralizado para el manejo de certificados, el cual siguiendo las mejores prácticas de la industria NIST SP 1800-16 "Protección de transacciones web: administración de certificados del servidor de seguridad de la capa de transporte (TLS)", se obtuvieron los siguientes logros: estandarizar el ciclo de vida de los certificados digitales, establecer un inventario de certificados digitales, reducir un total de 8800 certificados sin propietario a cero, es decir se identificaron quien es el propietario real, identificación de problemas y vulnerabilidades de la infraestructura de TLS y se

logró definir un mecanismo de monitoreo manual de certificados pronto a caducar. Aunque el avance en la solución es importante y significativo, aún queda mucho por mejorar para que el ciclo de vida del certificado sea mucho más ágil, y eliminar potencial error humano.

1.3 Definición y Descripción del Problema

Gracias al rápido avance en las tecnologías y al crecimiento exponencial en la infraestructura de las compañías, la gestión de la administración del ciclo de vida de los certificados digitales se ha convertido en un proceso crítico y retador para las compañías transnacionales de gran tamaño. En el entorno empresarial actual, muchos sistemas emplean comunicaciones a través de redes digitales como intranets e internet. Cuando se utilizan estos sistemas, la seguridad de las comunicaciones entre las partes siempre es una preocupación y se convierte en una prioridad. Contar con una comunicación encriptada, es crítico para una infraestructura segura, por lo que los certificados digitales se convierten en la herramienta principal para establecer un canal de comunicación seguro. La autoridad de certificación o autoridad certificadora es una entidad que emite certificados digitales para uso de otras partes, un ejemplo de un tercero de confianza es: Thawte, Comodo y Entrust (Jarvie et al., 2013).

Cuando una organización cuenta con múltiples servidores, estos pueden incluir varios mecanismos de seguridad que permiten que los servidores se comuniquen entre ellos de forma segura, por ejemplo, los certificados. La utilización de este método conlleva algunas consideraciones a tomar en cuenta como es la administración del ciclo de vida de los certificados y el detallado planeamiento requerido para la actualización de este mismo (Sharif et al., 2015).

Las grandes corporaciones pueden encontrarse administrando miles de certificados digitales, los cuales se encuentran en constante crecimiento. Cada uno de estos certificados digitales tienen un ciclo de vida que consta de solicitud de nuevos certificados, autorización para usar el certificado, administrar y uso del certificado, solicitud de reemplazo, renovación y eliminación de certificados expirados. La administración de los ciclos de vida se complica aún más por el hecho de que los certificados caducan un año después de su emisión, con la emisión de certificados que se producen de forma continua. Administrar decenas de miles de certificados que expiran de forma continua es una tarea ardua y compleja (Jarvie et al., 2013).

Un problema típico que ocurre con la gestión del ciclo de vida de los certificados es la dificultad de gestionar manualmente los certificados. Esto se debe a que las solicitudes de gestión de certificados, relacionadas al ciclo de vida de los certificados son típicamente a través de correo electrónico, lo cual puede conducir a una falta de responsabilidad o una falta de acción por parte del destinatario del correo electrónico (ejecutor de la acción) y no responder en la brevedad requerida o no responder por completo al correo (Jarvie et al., 2013).

Se ha identificado que una importante cantidad de incidentes mayores que causan interrupción grave a las actividades y operaciones del negocio son ocasionados a raíz del mal manejo del ciclo de vida de los certificados digitales para los miles de servidores y certificados en producción, como resultado de esto se pueden observar certificados expirados sin renovar, certificados instalados erróneamente, certificados sin propietarios asociados o propietarios que ya no están en la compañía o cambiaron de departamento, certificados sin aplicaciones asociados, certificados que deberían descontinuarse pero siguen activos. Actualmente no existe un

sistema o proceso robusto y efectivo que se asegure que los certificados pronto a expirar sean renovados a tiempo y con éxito, ocasionando que las operaciones diarias de diferentes grupos de negocios se vean impactados, ya que cualquier fallo de algún certificado significa la interrupción del servicio por un tiempo no estimado. Para organizaciones grandes, una interrupción importante podría resultar en cientos de miles o incluso millones de dólares en ingresos perdidos. Por lo tanto, existe la necesidad de una mejora en cuanto al monitoreo de la fecha de caducidad de los certificados. Se requiere garantizar que se emita un certificado correctamente y, una vez emitido, que el certificado sea instalado y configurado exitosamente en el servidor o dispositivo donde se utilizará (skarda et al., 2013).

El propósito de este proyecto es proponer estandarización y automatización de manera eficaz y eficiente la renovación de certificados digitales, y con esto eliminar potenciales incidentes mayores causados por certificados expirados o erróneamente instalados, ya que algunos certificados son complicados de instalar y configurar adecuadamente (skarda et al., 2013). Evitar el impacto negativo en los clientes debido a la expiración de certificados, mejorando la responsabilidad y reportar a tiempo a jefaturas, a través de la autoadministración y el alojamiento fechas certificados (Jarvie et al., 2013).

Para lograr tener una propuesta se pretende llevar a cabo una investigación de soluciones actuales para la administración y gestión del ciclo de vida de certificados digitales, enfocado en la renovación de certificados, para grandes compañías transnacionales.

En la actualidad se ha identificado que muchos de los desarrollares de aplicaciones de software no contemplan la gestión del ciclo de vida del certificado como parte de su lógica, esto debido a que carecen de familiaridad con las

funciones relacionadas con la seguridad. Por lo tanto, cuando un certificado y / o clave pública ha caducado, comprometerá la seguridad de los datos producidos por la aplicación de software (Hillier et al., 2000), y al mismo tiempo ocasionará que los sistemas de información fallen. El aumento en la utilización de certificados digitales en los sistemas de TI hace que el seguimiento a la fecha de expiración y el manejo de otros datos relacionados a estos se conviertan en un reto (Boniface et al., 2014). Debido a lo expuesto anteriormente es que existe la necesidad de una solución que administre el ciclo de vida de los certificados digitales, sin que las aplicaciones de software tengan que incluir la lógica de programación (Hillier et al., 2000).

1.4 Justificación

La importancia del presente proyecto radica en varias razones:

1. Lograríamos mayor eficiencia en el manejo del ciclo de vida de certificados digitales al disminuir las horas dedicadas a realizar implementaciones y configuraciones manuales de certificados digitales por parte de un ingeniero, Intel cuenta con un total de 11349 certificados activos a este momento, lo cual representa un ahorro de más de 11349 horas de trabajo manual por año.
2. Se elimina errores de configuración por medio de la automatización ya que garantizará la coherencia.
3. Se lograría contar con un mayor control y visibilidad de cómo y dónde se utilizan los certificados.
4. Se elimina monitoreo y seguimiento manual de certificados digitales pronto a expirar representando un ahorro de más de 260 horas de trabajo manual anual.
5. Se disminuye el riesgo de que ocurra algún suceso que pueda generar un impacto negativo económico y de imagen.

Adicionalmente un claro ejemplo del porque en la actualidad la gestión y manejo de certificados digitales se ha convertido en un proceso crítico para las compañías, fue lo sucedido a Equifax en el 2017, cuando fueron víctima de fuga de información personal financiera de 143 millones de consumidores de EE. UU, esto a raíz de que cibercriminales aprovecharon la vulnerabilidad Apache Struts CVE-2017-563 de una aplicación web de EE. UU y a que un certificado digital caducado contribuyó a la capacidad de los atacantes para comunicarse con servidores comprometidos y así robar datos sin ser detectados.

Esta investigación está enfocada en aportar una propuesta de mejora ágil en el sistema software gestor de certificados digitales Enterprise, mediante un proceso eficaz y eficiente que garantice la renovación de certificado a punto de caducar y con esto eliminar potenciales incidentes mayores causados por certificados expirados o certificados mal configurados.

1.5 Viabilidad

A continuación, se desarrolla el por qué este proyecto es viable, enfocándonos en el punto de vista técnico, operativo y económico.

1.5.1 Punto de Vista Técnico Como profesional informático, Licenciado en Ciencias de la Computación con énfasis en Administración y futuro Máster en ciberseguridad, he obtenido los conocimientos requeridos en el tema de criptografía, lo cual me dan las herramientas para poder llevar a cabo con éxito la presente investigación. Adicionalmente en mi posición laboral actual he adquirido experiencia en el ciclo de vida de los certificados digitales enterprise especialmente durante eventos de crisis, esto me ha permitido familiarizarme con esta tecnología, formar alianzas estratégicas y contar con el apoyo del departamento encargado de la infraestructura de PKI de Intel para futuras propuestas de mejora. Finalmente, con

la presente investigación se pretende recopilar el conocimiento necesario que ayuden a solventar los problemas expuestos.

1.5.2 Punto de Vista Operativo Para este proyecto se tiene planeado realizar un estudio de mercado de las herramientas a nivel enterprise lideres en la gestión de certificados digitales, para posteriormente una vez identificado la solución ideal hacer la propuesta y crear un manual técnico de cómo se configura la herramienta para la automatización de la renovación de certificados digitales. También es importante mencionar la administración del ciclo de vida de los certificados digitales ya forma parte de sus roles y responsabilidades, estas pruebas vienen a aportar agilidad al proceso y en caso de algún fallo de alguna tarea, esta se completará de la manera que normalmente se realiza. Por lo tanto, esta investigación no altera de ninguna manera el funcionamiento de las operaciones de la compañía o ninguno de los recursos utilizados.

1.5.3 Punto de Vista Económico Los costos de inversión estimada para el desarrollo de este proyecto son las horas de consultoría, las cuales se asumen como parte de la tesis.

Tabla 1*: Costo de horas consultor*

Investigador	Horas semanales	Total semanas (4 meses)	Total horas (4 meses)	Costo x hora	Costo Teórico Total
Romel Espinoza	25	36	900	10000	9,000,000

Fuente: Elaboración propia basada en Tusalario.com y mtss

Es importante aclarar que el proyecto es proponer una solución de software, para ello utilizaremos versiones de prueba para su evaluación, las cuales no tienen costos económicos. La adquisición del software a proponer queda a criterio de la compañía.

1.6 Objetivos

Para la definición del objetivo general y específico se utiliza la taxonomía de tipo jerárquico de Bloom, ya que se ha logrado demostrar su efectividad a través de los años, además de su amplio uso, en específico en el ámbito educativo costarricense.

1.6.1 Objetivo General Proponer una mejora ágil en el sistema software gestor de certificados digitales Enterprise para Intel.

1.6.2 Objetivos Específicos

- Identificar las principales fallas de la gestión y manejo del ciclo de vida, por medio de un examen sistemático del flujo, y demostrar al negocio cuales son los problemas que se pueden corregir y de qué manera se puede corregir.
- Investigar las mejores prácticas en el mercado sobre gestión y manejo del ciclo de vida de los certificados digitales Enterprise, a través de un benchmarking.
- Realizar un análisis profundo de las soluciones identificadas que agilice el ciclo de vida de los certificados digitales Enterprise, para así eliminar la causa raíz de la falla.
- Comparar los principales resultados que genera el análisis de las herramientas, para demostrar que la herramienta efectivamente elimina parcial o completamente los defectos de gestión detectados, los beneficios que se obtienen y concluir con una propuesta de solución.

1.7 Alcances y Limitaciones

1.7.1 Alcances

Los alcances del proyecto son:

- Creación de manual técnico para la automatización de la renovación de certificados digitales.

- La investigación se limita en sistemas operativos WINDOWS y servidores web IIS inicialmente.

- Al concluir el proyecto, los documentos resultantes de todo el proyecto, incluyendo la prueba de concepto, estaría disponible para la población en general de Intel.

- Un portal, y manual de usuario con información y ayuda necesaria.

1.7.2 Limitaciones

Las limitaciones del proyecto son:

- El presente proyecto al ser una propuesta, no se contempla implementar el software en producción para uso general, ya que la adquisición del software queda a criterio de la compañía.

- Los escenarios y criterios que quedan excluidos de la prueba de concepto son: sistemas operativos distribuidos Linux, certificados para aplicaciones PHP, Certificados manejados por load balancers y páginas web fuera del firewall de Intel.

- Para efectos de esta investigación solo se tomarán en cuenta soluciones que por sus características se considera pueden aportar valor agregado a la organización.

1.8 Marco de Referencia Organizacional y Socioeconómico

1.8.1 Historia

La corporación Intel es una compañía estadounidense, fundada en Mountain View (California) en el año de 1968 por Gordon E. Moore y Robert Noyce como Integrated Electronics Corporation. Inicio creando el corazón de calculadoras, y a través de los años se ha mantenido como una empresa importante en lo que a microprocesadores se refiere. Aunque Intel dominaba el mercado de los microprocesadores, ya que en la actualidad el principal competidor de Intel en el mercado es Advanced Micro Devices (AMD); sigue siendo catalogada líder mundial en fabricación de circuitos integrados.

A continuación, listamos algunos de los momentos más importantes de la compañía en sus 52 años de existencia que nos ayudan a entender su importancia en la historia de la computación:

- 18 de Julio de 1968: Robert Noyce y Gordon Moore establecen NM Electronics, poco después renombrada a Intel Corporation.
- Abril de 1969: Intel lanza la memoria de acceso aleatorio estática 3101 (SRAM), su primer producto.
- 1969: Intel lanza la 1101, la primera RAM estática de semiconductores de óxido de metal (MOS).
- 1971: Intel crea el 4004, el primer microprocesador.
- 1971: Intel presenta la memoria programable borrable (EPROM).
- 31 de octubre de 1971: Intel sale a bolsa con la oferta pública inicial.
- 1972: Intel abre la primera instalación de fabricación internacional en Penang, Malasia.
- 1973: Intel abre una fábrica de obleas en Livermore, California, la primera fuera de Silicon Valley.
- 1974: Intel lanza el microprocesador 8080 de 8 bits.
- 1976: Intel estrena la familia de microcontroladores MCS-48.
- 1978: Intel lanza el procesador 8086, el primer procesador de 16 bits y el primero basado en la arquitectura x86.
- 1979: Intel encabeza la lista Fortune 500.
- 1981: IBM selecciona el microprocesador 8088 de Intel para el IBM PC, el primer ordenador personal.
- 1982: Intel lanza el primer procesador 286, el 80286 de 16 bits.

- 1983: Intel supera los 1.000 millones de dólares en ingresos.
- 1985: Intel presenta el procesador 386, un chip de 32 bits.
- 1988: Se crea la Fundación Intel.
- 1991: Arranca la campaña de mercadotecnia Intel Inside.
- 1993: Intel presenta el procesador Pentium.
- 1995: Intel colabora en la especificación USB, el gran estándar mundial para conexión de periféricos.
- 1997: Time Magazine nombra a Andy Grove su «Hombre del año».
- 1999: Intel entra en el Dow Jones Industrial.
- 2003: Intel lanza los procesadores Centrino, integrando un procesador móvil, conjuntos de chips relacionados y funciones de red inalámbrica 802.11.
- 2007: Intel produce procesadores que usan transistores de 45 nanómetros.
- 2011: Intel anuncia la especificación para computadoras portátiles Ultrabook.
- 2016: Intel se reestructura de una empresa centrada en PCs a una empresa centrada en datos.
- 2017: Intel desarrolla chips que usan transistores fabricados en procesos tecnológicos de 10 nm.
- 2018 Intel cumple 50 años de existir en el mercado.

1.8.2 Tipo de Negocio y Mercado Meta

La corporación Intel diseña, fabrica y vende circuitos integrados para la industria de la computación y las comunicaciones a nivel mundial. Su cartera de productos incluye microprocesadores, chipsets, tarjetas madre y conectividad con y sin cables.

1.8.3 Misión, Visión y Valores

Visión.

Ser el líder de desempeño confiable que libera el potencial de los datos.

Misión.

Diseñamos soluciones para los mayores desafíos de nuestros clientes con computación confiable desde la nube hasta el borde, inspirados en la Ley de Moore.

Valores.

Obsesionado por el cliente, un solo Intel, intrépido, verdad y transparencia, inclusión y calidad.

1.8.4 Políticas Institucionales

Una política es una declaración de cómo se debe usar y manejar los datos, ya sea externa o internamente. Una política refleja objetivos, reglas y requisitos formales, pero de alto nivel que cambian con poca frecuencia. Se requiere una aprobación especial cuando una persona desea tomar un curso de acción que no cumple con la política.

Las políticas pueden estar respaldadas por procedimientos, pautas, manuales, estándares, etc.

1.8.4.1 Política de Confidencialidad de los datos de Intel

Intel Confidential (IC) significa información de Intel que no es pública, por lo tanto, es importante protegerla, pero no requiere el nivel más alto de controles. IC incluye la mayor parte de la información comercial, financiera y legal, así como la información

técnica que necesita un cliente para completar un diseño basado en un producto Intel, o información que se revelaría mediante ingeniería inversa de un producto Intel lanzado.

Específicamente en el área de la tecnología, Intel consideran los siguientes datos como confidenciales:

- Interfaces de programación de hardware a software (por ejemplo, para controladores)
- Especificaciones de arquitectura de software
- Documentos de diseño de software de alto nivel
- Manuales de referencia del programador
- Documentación de procesos internos para software
- Especificaciones del BIOS y pautas de ajuste
- Guías del escritor de BIOS
- Código de inicialización de CPU
- Código de inicialización de Platform Controller Hub
- Código de referencia de memoria
- Código de referencia (BIOS, firmware, controladores)
- Código de muestra (BIOS, firmware, controladores)
- Firmware del producto
- Validaciones de software
- Pruebas de compatibilidad y vulnerabilidad.
- Kits de desarrollo de software
- Herramientas de desarrollo de software que permiten a los clientes desarrollar, analizar o depurar sus diseños utilizando productos Intel.

- Tecnología de arranque rápido de software
- SaaS

1.8.4.2 Política en ciberseguridad

El Congreso debe apoyar el enfoque del Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) para mejorar la ciberseguridad. Intel elogia a la administración y al NIST por construir el marco de ciberseguridad de la mano con la industria y otras partes interesadas para construir un modelo de herramienta voluntaria basada en riesgos que puede ser utilizada por una amplia gama de organizaciones del sector público y privado.

1.9 Estado de la Cuestión

La presente propuesta de mejora tiene como finalidad recopilar conocimiento con respecto a las mejores prácticas en el mercado sobre manejo del ciclo de vida de los certificados digitales Enterprise, se dará mayor enfoque a publicaciones con data reciente, que nos aporte una base para una investigación más profunda e innovadora. El estado de la cuestión será basado en la plantilla de Biolchini para una revisión sistemática.

La herramienta utilizada en esta investigación ha sido el de revisión bibliográfica, el cual consiste en búsquedas intensivas del tema a tratar mediante múltiples fuentes de información, para este caso solo fueron consultadas fuentes digitales.

1.9.1 Planificación de la revisión

1.9.1.1 Formulación de la pregunta

La formulación de la pregunta nos ayuda a dar un refinamiento y enfoque al tema y subtemas de investigación, para una mejor y efectiva búsqueda de las publicaciones.

1.9.1.1.1 Formulación de la pregunta

Se requiere realizar búsquedas de publicaciones enfocadas en el área de la administración ágil de los certificados digitales corporativos, estos deben aportar innovación y automatización, específicamente en la renovación de estos.

1.9.1.1.2 Amplitud y calidad de la pregunta

Problema: En compañías transnacionales grandes donde el inventario de servidores con certificados digitales es tan grande, y que se mantiene en constante crecimiento, la administración de estos se ha convertido en un reto.

Pregunta: Con base en la descripción de la problemática anterior la pregunta de investigación es: ¿Qué propuestas de solución existen para gestión ágil de certificados digitales para grandes compañías?

Palabras clave y sinónimos: A continuación, se lista todas las posibles palabras claves que nos ayude a encontrar artículos y publicaciones entorno a la temática de investigación.

Tabla 2: *Listado de palabras.*

Palabra en Ingles	Palabra en español
digital certificate	Certificados digitales
certificate management	gestión de certificados
digital certificate lifecycle	Ciclo de vida de Certificados digitales
digital certificate management	Gestión de Certificados digitales

Automated certificate management	Gestión de certificados automatizado
Certificate renewer	Renovador de certificados

Fuente: Elaboración propia.

Intervención: El contexto de la revisión sistemática se planea extraer los artículos y publicaciones de mayor relevancia acerca de propuestas sobre gestión y automatización del ciclo de vida de los certificados digitales corporativos.

Control: En la presente propuesta de investigación no se cuenta con material bibliográfico inicial.

Efectos: Se espera obtener bibliografía de investigaciones previas de propuestas de mejora y automatización de software de gestión del ciclo de vida de certificados corporativos para para posteriormente analizarlas, compararlas e identificar necesidades de investigación u oportunidades de mejora.

Medidas de salida: Como medida de resultado se espera encontrar múltiples investigaciones de propuestas existentes para el manejo de Certificados Digitales corporativos

Población: Cualquier publicación sobre certificados digitales e infraestructura.

Aplicación: Corporaciones transnacionales donde existen inventarios de certificados digitales muy grande.

Diseño experimental: En el diseño experimental se utilizan los conocimientos previos de publicaciones encontradas como base, para una evaluación del estado actual, para poder detectar deficiencias, y posteriormente proponer posibles áreas de mejora e innovación.

1.9.1.2 Selección de fuentes

Definición del criterio de selección de fuentes: La selección de las fuentes está basada en varios factores: relación del tema del articulo con la presente investigación, dominio del tema en investigación por parte del autor de la presente investigación y popularidad de la fuente, adicionalmente tienen que ser fuentes donde el acceso a las bibliotecas de publicaciones web sea libre y que se puedan realizar búsquedas avanzadas.

Lenguaje de estudio: El idioma principal de búsqueda es el inglés y como segunda opción español.

Identificación de fuentes:

Métodos de búsqueda: La ejecución de las búsquedas para los estudios primarios de la presente investigación se realiza por medio de motores de búsqueda especializados. Adicionalmente se consulta a expertos en el área sobre fuentes que pueda aportar conocimiento.

Lista de fuentes: La selección de las fuentes más relevantes y utilizadas para la ejecución de la revisión sistemática están:

Scholar Google

Research Gate

IEEE xplore DIGITAL LIBRARY

Springer

Academia

Cadena de Búsqueda: Para la selección de los datos se utilizaron los siguientes criterios de búsqueda:

¨digital certificate lifecycle ¨ or intitle:” digital certificate lifecycle”

¨digital certificate management¨ or intitle: ¨digital certificate management¨

Intitle:"digital certificate"

Intitle: "public key" +"lifecycle"

Intitle:"digital certificate" +"lifecycle"

digital certificate +"lifecycle"

systems for automated authentication digital certificates

digital certificates systems for dynamic updates

digital certificates systems and methods

digital certification technological infrastructure

Selección de fuentes después de la evaluación: Las variables para seleccionar las fuentes a utilizar fueron: amigable para realizar cadenas de búsqueda y que los resultados sean documentos de buena calidad.

Comprobación de las fuentes: Las fuentes a utilizar fueron seleccionadas en base a recomendaciones de expertos en el área de investigación académica.

1.9.1.3 Selección de los estudios

En este apartado se describe el criterio final de inclusión y exclusión de las publicaciones previamente identificadas, y seleccionar las publicaciones relevantes para análisis final.

Definición del criterio de inclusión y exclusión de estudios: Se tomarán en cuenta los estudios que apliquen algoritmos de automatización para la gestión del ciclo de vida de certificados digitales, productos de plataforma software comercial. Se excluirán los estudios con temáticas alrededor de arquitectura, encriptación y llaves públicas/privadas.

Procedimiento para selección de estudios: Una vez definido los criterios de inclusión y exclusión, la selección de los estudios se realiza de la siguiente manera: Paso número uno se realiza la lectura del resumen, paso número dos se continua con la

Introducción, y paso número tres conclusiones. Si estas tres lecturas breves nos dan un resultado positivo se continua con la lectura completa del artículo, de lo contrario el artículo se descarta, tal y como se muestra en la figura #1 a continuación.

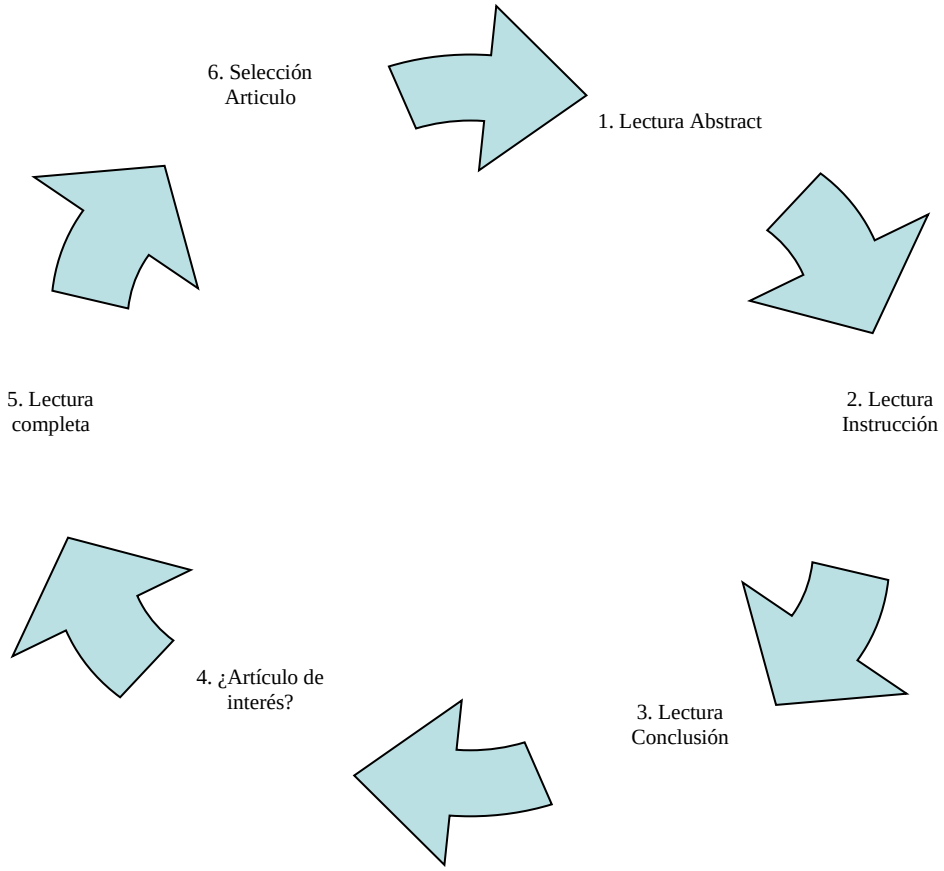


Fig. 1 Método de selección de artículos.

Fuente elaboración propia

1.9.2 Ejecución de la revisión

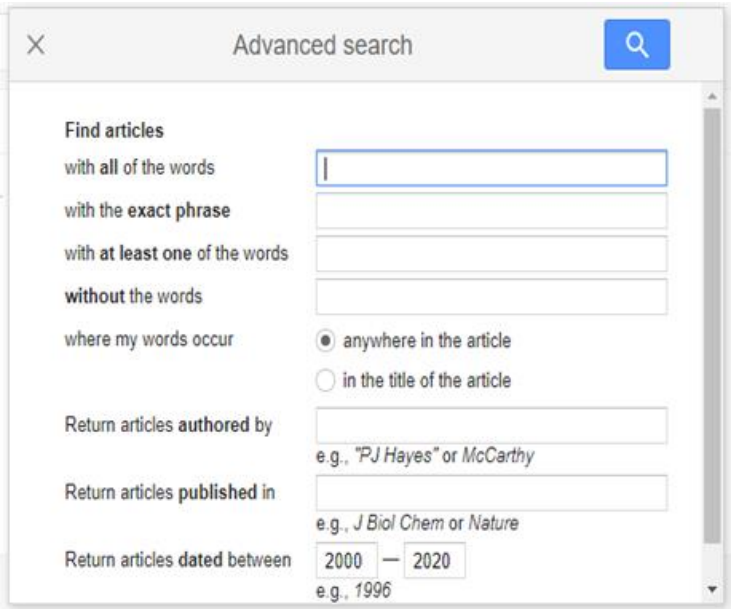
Una vez se tiene definido como se va a realizar la búsqueda, las fuentes de búsqueda a utilizar, las cadenas de búsquedas y los criterios de inclusión y exclusión el siguiente paso es ejecutarlas. También es importante mencionar que la recopilación de la información incluye papers, investigaciones finales de graduación

y páginas web de software comercial, los cuales no da un valioso aporte al tema de investigación.

1.9.2.1 Ejecución de la selección en la fuente Google Scholar

1.9.2.1.1 Selección de estudios iniciales

Para la búsqueda inicial, primero limitamos los años de publicación de las literaturas en la opción de búsqueda avanzada:



En las siguientes tablas se muestra los documentos seleccionados e investigados, se utiliza las cadenas de búsquedas definidas en el punto 1.9.1.2 apartado cadena de búsqueda, luego se aplica los criterios de inclusión y exclusión, da como resultado los siguientes documentos:

Tabla 3: *Publicaciones seleccionadas Google Scholar.*

Título	Autores	Año
Digital Certificate Management	Boniface, R., Randall, M., & friendman, J.	2014
Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices	Chokhani, S., Ford, W., Sabett, R., Merrill, C., & Wu,	2003

Framework	S.	
Method and apparatus for centralizing processing of key and certificate life cycle management	Hillier, S., Lee Dilkie, R., & Rosenquist, G.	2000
Method and system for pluggability of federation protocol runtimes for federated user lifecycle management	Hinton, H. M., Falola, D. M., Moran, A. S., & Wardrop, P. R.	2010
Systems and methods for managing digital certificates	Jarvie, J., Vayner, L., & Payne, C.	2013
Automated Certificate Management	Sharif, T., Brace, C., & Garg, N.	2015
Method for creating and installing a digital certificate	Skarda, C.	2013

Fuente: Elaboración propia.

1.9.2.1.2 Evaluación de la calidad de los estudios

Todos los documentos listados son patentes estadounidenses, confirmando así su calidad.

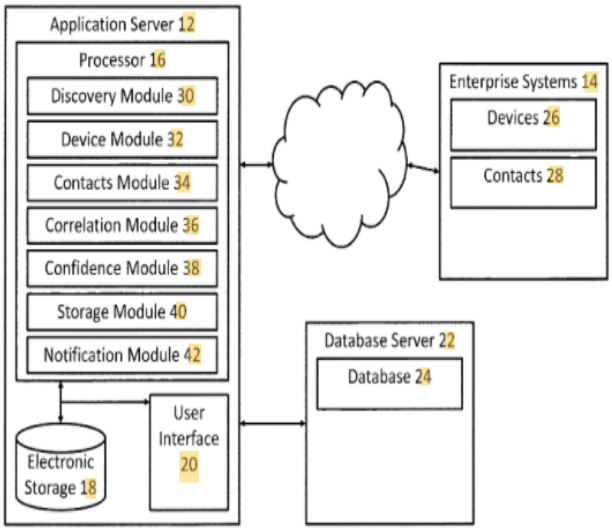
1.9.2.1.3 Revisión de la selección

Este apartado se lleva a cabo tras la lectura y revisión de: 1- abstract, 2- introducción, 3- conclusión y 4- finalmente el contenido completo de cada documento.

1.9.2.1.4 Extracción de información

Tabla 4: *Publicación #1*

Identificación	Publicación #1
Título	Digital Certificate Management
Publicación	2014
Autores	Boniface, R., Randall, M., & friendman, J.
Descripción	
Área	- Mecanismos criptográficos para comunicaciones secretas o seguras - Arquitecturas de red para la seguridad de la red
Resumen	Este documento se refiere a un sistema de gestión de certificados digitales configurado para consolidar la información relacionada con los certificados digitales en los sistemas empresariales.
Aspectos a destacar	
	Ilustra un sistema de gestión de certificados digitales configurado para consolidar la información relacionada con los certificados digitales en los sistemas empresariales

Identificación	Publicación #1
	 FIG. 1 Muestra listas de ejemplo de posibles parámetros de certificados digitales, herramientas de descubrimiento de certificados, parámetros de dispositivos, herramientas de descubrimiento de dispositivos, parámetros de contacto y posibles herramientas de descubrimiento de contactos.

Identificación	Publicación #1

200 Digital Certificate Parameter Examples
Algorithm ID
Extensions
Issuer
Issuer Unique Identifier
Public Key Algorithm
Serial Number
Signature
Signature Algorithm
Subject
Subject Public Key
Subject Unique Identifier
Validity Not After
Validity Not Before
Version

202 Example Certificate Discovery Tools
802.11X Authentication Systems
Agent-Based Certificate Scanners
Certificate Authorities
Network Mapping Scanners
Network-Based Certificate Scanners
Vulnerability Assessment Scanners
Wired Network Control Systems
Wireless Network Control Systems

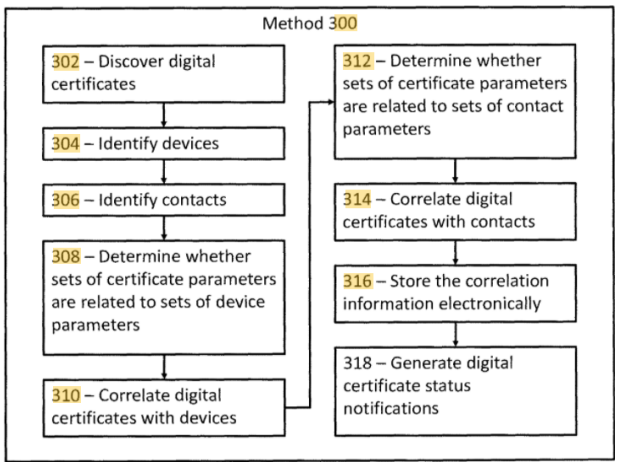
204 Device Parameter Examples
Common Name
DNS Name
IP Address(es)
Last Seen
Last Used
Logical Location
MAC Address(es)
NetBIOS Name
Owning Approval Group
Owning Segment or Business Unit
Owning Support Group
Physical Location
Related Application(s)

206 Example Device Discovery Tools
802.11X Authentication Systems
Active Directory
Anti-Malware Detection Systems
Configuration Management Databases
Network Mapping Scanners
Network-Based Certificate Scanners
Rogue Device Detection Systems
Software Distribution Systems
Vulnerability Assessment Scanners
Wired Network Control Systems
Wireless Network Control Systems

208 Contact Parameter Examples
Address(es)
Cost Center
Department
E-Mail Address(es)
Employee ID
Name(s)
Privileges (related to CIPHER)
Reporting Hierarchy
Status
Telephone Number(s)
Time Zone
User ID(s)

210 Example Contact Discovery Tools
Active Directory
Contractor Directories
Employee Directories
Incident/Call Tracking Systems
Organization Charts
SAP
Telephone Directories
Vendor Directories

Ilustra un método para consolidar información relacionada con certificados digitales de todos los sistemas empresariales.



Fuente: Elaboración propia.

Tabla 5: *Publicación #2*

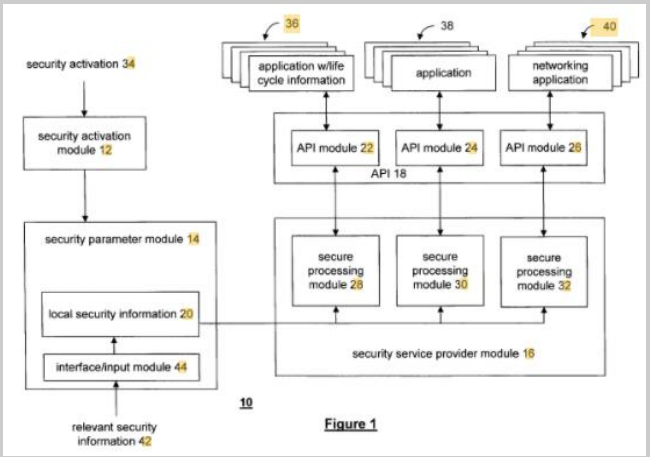
Identificación	Publicación #2
Título	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
Publicación	2003
Autores	Chokhani, S., Ford, W., Sabett, R., Merrill, C., & Wu, S.
Descripción	
Área	- Política de certificados - Declaración de prácticas de certificación
Resumen	El propósito de este documento es doble. Primero, el documento tiene como objetivo explicar los conceptos de un CP y un CPS, describir las diferencias entre estos dos conceptos, y describe su relación. En segundo lugar, este documento tiene como objetivo presentar un marco para ayudar a los redactores y usuarios de certificados políticas o CPS en la redacción y comprensión de estos documentos. En particular, el marco identifica los elementos que pueden necesitar ser considerado en la formulación de un CP o un CPS. El propósito no es definir políticas de certificados particulares o CPS, per se.
Aspectos a destacar	
	Este marco describe el contenido de un

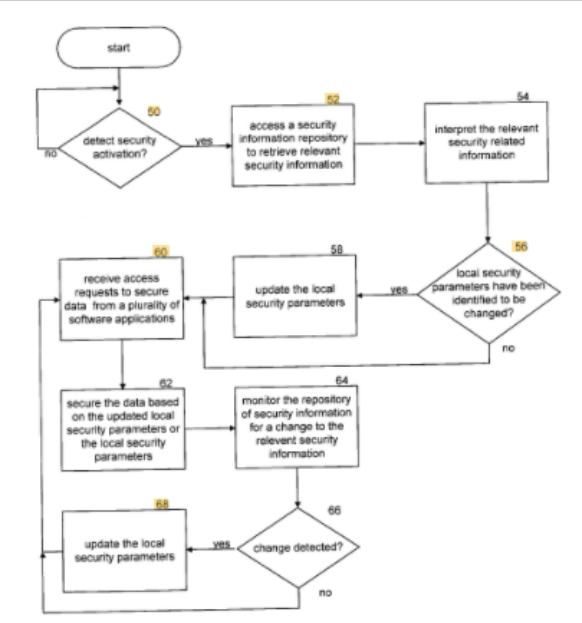
Identificación	Publicación #2
	conjunto de disposiciones, en términos de nueve componentes primarios, como sigue: 1. Introducción 2. Publicación y repositorio 3. Identificación y autenticación 4. Requisitos operativos del ciclo de vida del certificado 5. Instalaciones, gestión y controles operativos 6. Controles técnicos de seguridad 7. Certificado, CRL y perfil OCSP 8. Auditoría de cumplimiento 9. Otros asuntos comerciales y legales

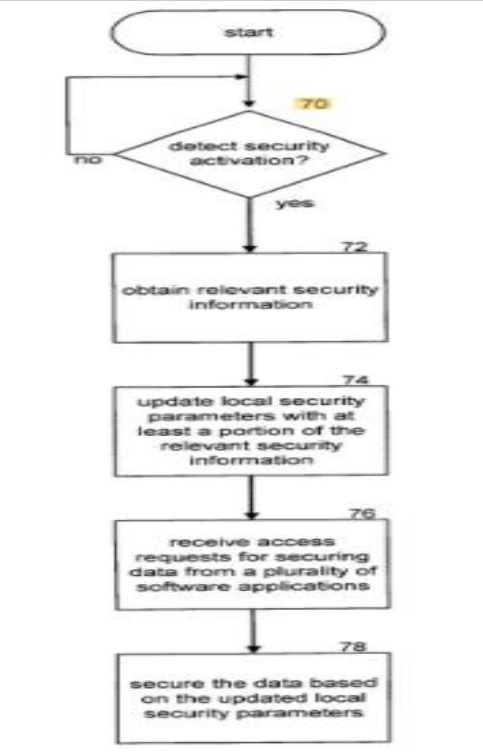
Fuente: Elaboración propia.

Tabla 6: *Publicación #3*

Identificación	Publicación #3
Título	Method and apparatus for centralizing processing of key and certificate life cycle management
Publicación	2000
Autores	Hillier, S., Lee Dilkie, R., & Rosenquist, G.
Referencia	5,633,933 5/1997 Aziz ..... 380/30 5,825,300 10/1998 Bathricket al. … 340/825.33 5,864,667 1/1999 Barkan ..... 395/187.01 5,872,849 2/1999 Sudia ..... 380/49 5,922,074 7/1999 Richard et al. … 713/200

Identificación	Publicación #3
	5,935,246 8/1999 Benson 713/200
Descripción	
Área	- Autenticación de usuario - Llave pública, llave asimétrica, cifrado asimétrico
Resumen	La presente invención se refiere en general a comunicaciones seguras y más en particular a centralizar la gestión de claves y ciclos de vida de certificados.
Aspectos a destacar	
	Ilustra un diagrama de bloques esquemático de un dispositivo de comunicación seguro de acuerdo con la presente invención.  Ilustra un diagrama lógico de un método para procesar la clave y el certificado y la gestión del ciclo de vida

Identificación	Publicación #3
	 Ilustra un diagrama lógico de un método alternativo para procesar la gestión del ciclo de vida de claves y certificados

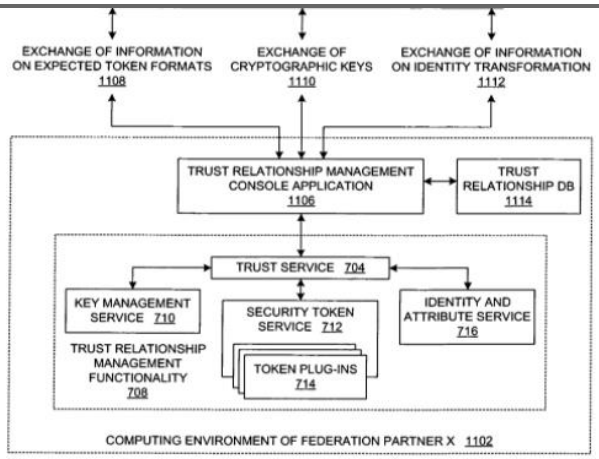
Identificación	Publicación #3
	

Fuente: Elaboración propia.

Tabla 7: *Publicación #4*

Identificación	Publicación #4
Título	Method and system for pluggability of federation protocol runtimes for federated user lifecycle management
Publicación	2010
Autores	Hinton, H. M., Falola, D. M., Moran, A. S., & Wardrop, P. R.
Descripción	
Área	Arquitecturas de red o protocolos de comunicación de red para la seguridad de la red para

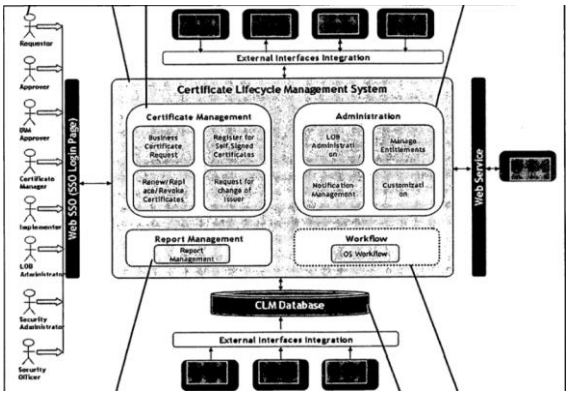
Identificación	Publicación #4
	respaldar la autenticación de entidades que se comunican a través de una red de paquetes de datos utilizando certificados
Resumen	La presente invención se refiere a un sistema de procesamiento de datos mejorado y, en particular, a un método y aparato para la transferencia de datos a múltiples computadoras. Aún más particularmente, la presente invención está dirigida a sistemas informáticos en red.
Aspectos a destacar	
	La construcción de una relación de confianza relación puede implicar el uso de información existente para la empresa del usuario administrativo, como claves privadas existentes, certificados digitales, tokens, información de mapeo de identidad, etc.; el usuario administrativo podría configurar el resto de la relación de confianza utilizando información conocida para el socio de confianza si está disponible, por ejemplo, claves públicas, certificados, información de mapeo de identidad, etc.

Identificación	Publicación #4
	

Fuente: Elaboración propia

Tabla 8: *Publicación #5*

Identificación	Publicación #5
Título	Sistemas y métodos de gestión de certificados digitales
Publicación	2013
Autores	Jarvie, J., Vayner, L., & Payne, C.
Descripción	
Área	- Seguridad digital - Sistemas y métodos de gestión de certificados digitales.
Resumen	Un método para administrar un certificado digital por un sistema informático puede incluir los pasos de recibir, en el sistema informático, una solicitud de un certificado digital de un solicitante y transmitir, por el sistema informático, la solicitud a un primer aprobador.

Identificación	Publicación #5
Aspectos a destacar	
	Es un diagrama muestra el flujo de información a través de un sistema de gestión de certificados, de acuerdo con ciertas realizaciones de la invención. 

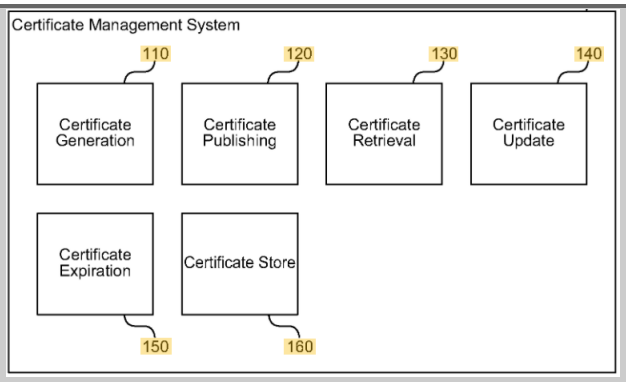
Fuente: Elaboración propia

Tabla 9: *Publicación #6*

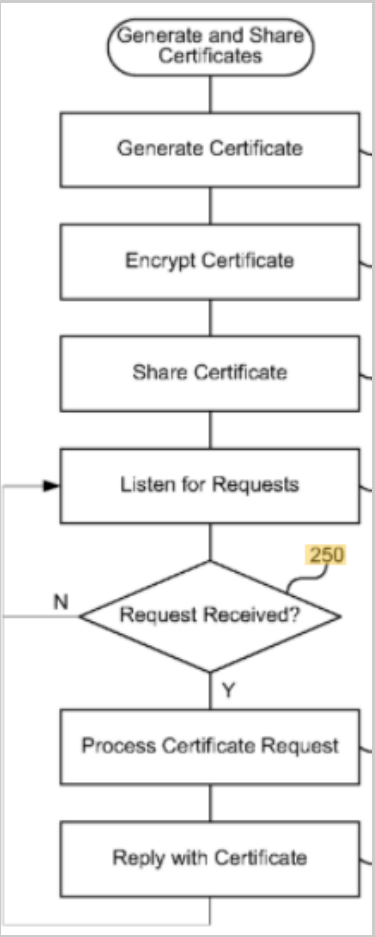
Identificación	Publicación #6
Título	Gestión de certificados automatizado
Publicación	2015
Autores	Sharif, T., Brace, C., & Garg, N.
Referencia	
Descripción	
Área	- Arquitecturas de red o protocolos de comunicación de red para la seguridad de la red para respaldar la autenticación de entidades que se comunican a través de una red de paquetes de datos utilizando certificados - Autenticación de usuarios mediante certificados

Identificación	Publicación #6
	- Perfiles de entidad - Arquitecturas de red o protocolos de comunicación de red para la seguridad de la red para soportar la gestión de llaves en una red de paquetes de datos para el intercambio de llaves.
Resumen	En este documento se describe un sistema de gestión de certificados que proporciona una gestión automatizada de los ciclos de vida y la distribución de certificados. En lugar de depender de un administrador u otro usuario para distribuir y administrar manualmente los certificados, el sistema de administración de certificados autogenera certificados, distribuye los certificados a los servidores apropiados u otras partes, y realiza la transición de certificados antiguos a certificados nuevos de una manera bien definida que evita romper la funcionalidad.
Aspectos a destacar	
	Es un diagrama que ilustra los componentes del sistema de gestión de certificados, en una realización.

Identificación	Publicación #6

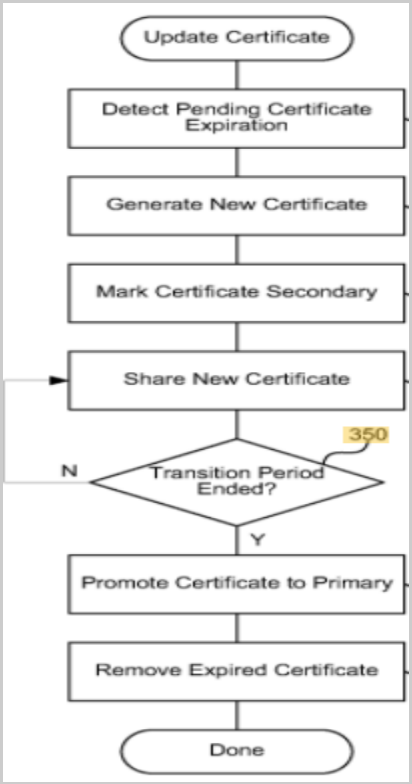


Es un diagrama de flujo que ilustra el procesamiento del sistema para generar y compartir certificados.



Es un diagrama de flujo que ilustra el

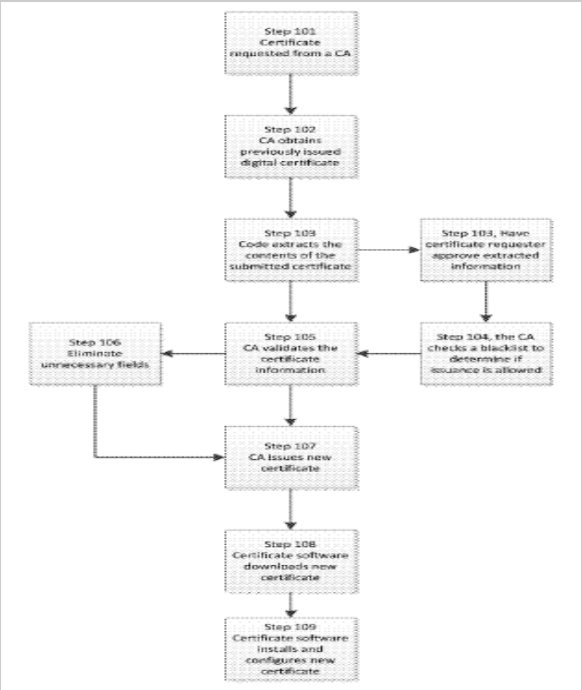
Identificación	Publicación #6
	procesamiento del sistema para actualizar uno o más certificados, en una realización.

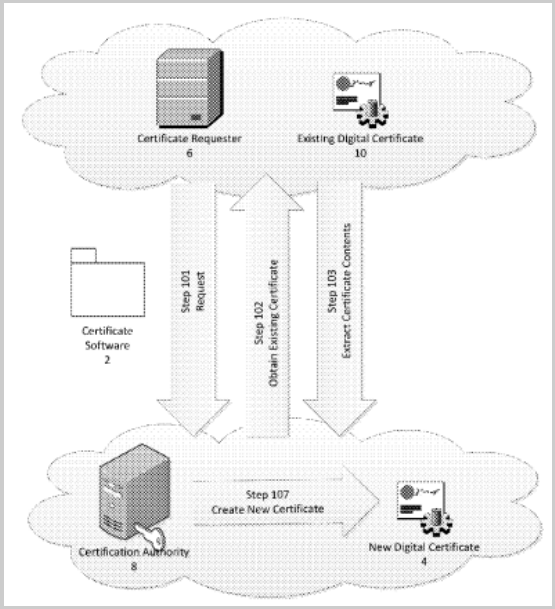
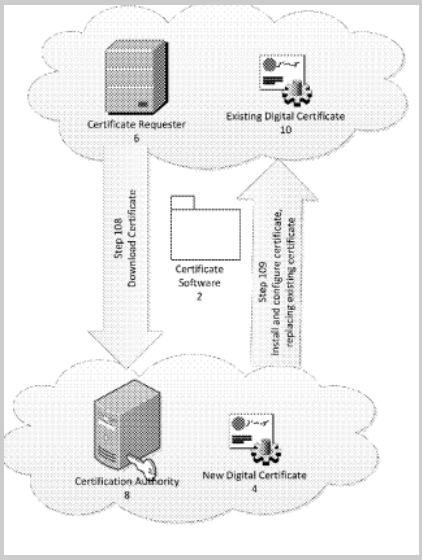


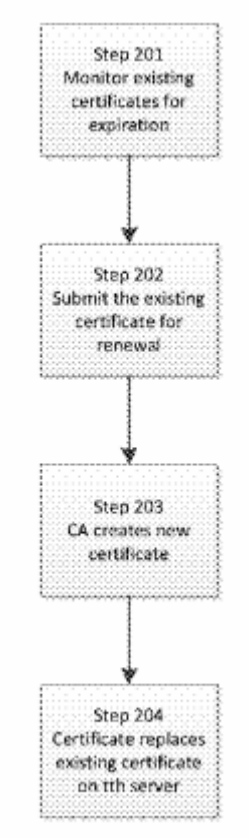
Fuente: Elaboración propia

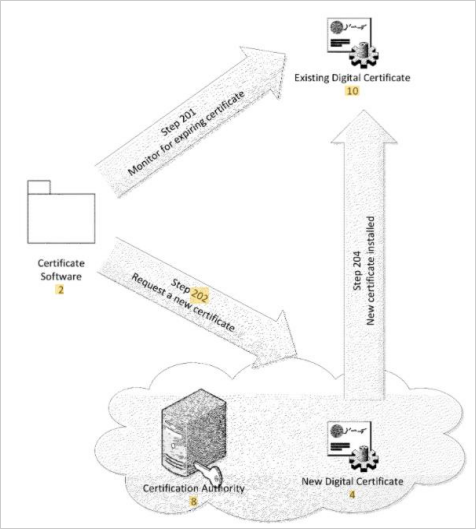
Tabla 10: *Publicación #7*

Identificación	Publicación #7
Título	Método para crear e instalar un certificado digital
Publicación	2013
Autores	Skarda, C.
Descripción	
Área	- Autenticación de usuarios mediante certificados - Arquitecturas de red o protocolos de comunicación de red para la seguridad de la red

Identificación	Publicación #7
	para respaldar la autenticación de entidades que se comunican a través de una red de paquetes de datos utilizando certificados
Resumen	La invención comprende un método para crear un certificado basado en el contenido de otro certificado. El certificado se instala y configura automáticamente en el servidor donde se utilizará. Una mejora adicional solicita e instala automáticamente el certificado antes de la expiración de un certificado existente.
Aspectos a destacar	
	Es un diagrama de flujo del proceso utilizado para crear e instalar un nuevo certificado digital. 

Identificación	Publicación #7
	Es un diagrama de cómo los componentes de la invención interactúan durante la solicitud y la creación del certificado procesado.  Es un diagrama de cómo los componentes del invención interactúa durante el proceso de instalación del certificado. 

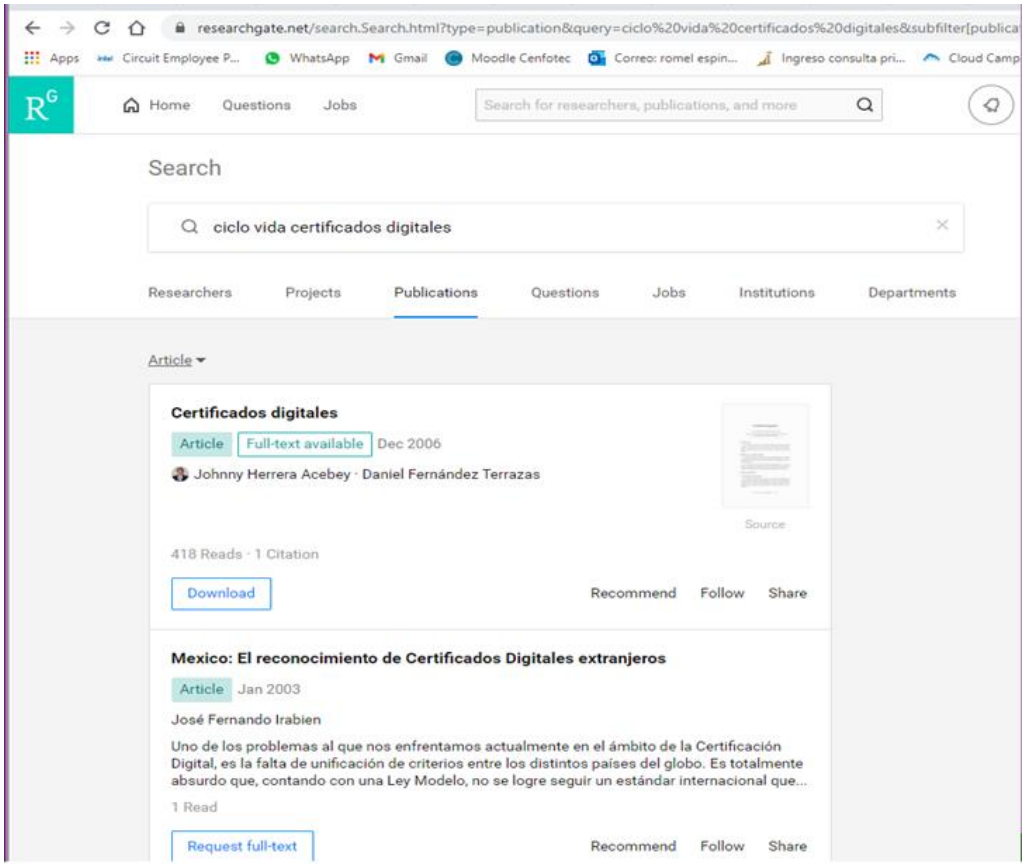
Identificación	Publicación #7
	Es un diagrama de flujo de una realización alternativa de la invención donde se solicita y emite un certificado automáticamente.  Es un diagrama que muestra cómo los componentes interactuar al solicitar y emitir un certificado automáticamente

Identificación	Publicación #7
	

1.9.2.2 Ejecución de la selección en la herramienta researchgate.net

1.9.2.2.1 Selección de estudios iniciales

Para la búsqueda inicial, se filtró por únicamente artículos publicados:



En las siguientes tablas se muestra los documentos seleccionados e investigados, se utiliza las cadenas de búsquedas definidas en el punto 1.9.1.2 apartado cadena de búsqueda, luego se aplica los criterios de inclusión y exclusión, da como resultado los siguientes documentos:

Tabla 11: *Publicaciones seleccionadas researchgate.net.*

Título	Autores	Año
Certificados digitales	Herrera, J., & Fernández, D.	2006
PKI* y firmas digitales: aplicaciones reales	Armando Carvajal	2007

Fuente: Elaboración propia

1.9.2.2.2 Evaluación de la calidad de los estudios

Todos los documentos listados son patentes estadounidenses, confirmando así su calidad.

1.9.2.2.3 Revisión de la selección

Este apartado se lleva a cabo tras la lectura y revisión de: 1- abstract, 2- introducción, 3- conclusión y 4- finalmente el contenido completo de cada documento.

1.9.2.2.4 Extracción de información

Tabla 12: *Publicación #8*

Identificación	Publicación #8
Título	Certificados digitales
Publicación	2006
Autores	Johnny Herrera Acebey Daniel Fernández Terrazas
Descripción	
Área	Certificados digitales

Identificación	Publicación #8
Resumen	Los sistemas que ofrecen servicios mediante Internet requieren de confianza, privacidad y seguridad entre ellos y sus clientes. El problema de la identificación de personas o sistemas que usan medios de comunicación no fiables se puede resolver usando certificados digitales.
Aspectos a destacar	
	En este artículo se presenta un estudio de los certificados digitales.

Fuente: Elaboración propia

Tabla 13*: Publicación #9*

Identificación	Publicación #9
Título	PKI* y firmas digitales: aplicaciones reales
Publicación	2007
Autores	Armando Carvajal
Descripción	
Área	Seguridad de la información en los negocios electrónicos
Resumen	El artículo describe las características mínimas que debe tener el comercio electrónico, luego muestra filosóficamente las diferencias entre la criptografía simétrica y la asimétrica, describe en detalle los certificados digitales, pero no hace una descripción matemática de la criptografía necesaria para su

Identificación	Publicación #9
	funcionamiento
Aspectos a destacar	
	Se selecciona la alternativa OpenCA por las siguientes razones: • Posee un API que puede ser utilizado desde los lenguajes de desarrollo de software para que el programador pueda mejorar sus propias interfaces de gestión, el resto de los proveedores evaluados no muestran la existencia de un API, para que el implementador mejore las características de cada opción. • En general, las opciones evaluadas no poseen soporte local lo que generaría dependencia tecnológica de estos proveedores que, en la mayoría de los casos, están en otros continentes, en cambio OpenCA por ser de tipo OpenSource permite que localmente se mejore la documentación y se hagan cambios específicos para la región, esto la hace una opción altamente deseable, según los requerimientos anteriormente enunciados. • Por ser OpenCA de licencia OpenSource no tiene costo de adquisición, sí hay costos de implementación y capacitación interna para aprender a manejar la herramienta.

Identificación	Publicación #9
	• Con OpenCA la curva de aprendizaje, es más larga que la de los productos ya establecidos en otros países que ya tienen documentación y soporte probado en sus países de origen. • Definitivamente los precios de los certificados individuales y la poca integración con las aplicaciones es lo que ha hecho difícil la implementación de PKI pues, finalmente, es el usuario quien paga estos costos. • Es una oportunidad única para aportar soluciones a la región en el tema específico de PKI con OpenCA

Fuente: Elaboración propia

1.9.3 Resumen de los resultados

La siguiente tabla #14 resume los artículos que fueron estudiados y analizados, para luego según su contenido y relación con el tema de estudio ser seleccionados como conocimiento base del presente proyecto de investigación.

Tabla 14*: Análisis de resultados*.

Fuente	Estudios	Relevantes	Primarios
Scholar Google	50	20	7
Research Gate	30	15	2
IEEE xplore	10	5	0
Springer	7	5	0
Academia	3	0	0

Fuente: Elaboración propia

Capítulo 2. Marco Conceptual

Para el desarrollo del marco conceptual utilizamos una nube de palabras sobre el contenido de la sección estado de la cuestión, esta nube nos permite identificar conceptos repetitivos que son importantes de aclarar para la presente investigación.

La figura a continuación muestra el resultado de la nube de palabras mencionada.

Fig. 2 Nube de palabras utilizando herramienta nubedepalabras.es.

Fuente: Elaboración propia

En el siguiente mapa conceptual jerárquico se muestra las palabras seleccionadas, basadas en el criterio:

1. Su recurrencia.
2. Relación directa con el tema de investigación.

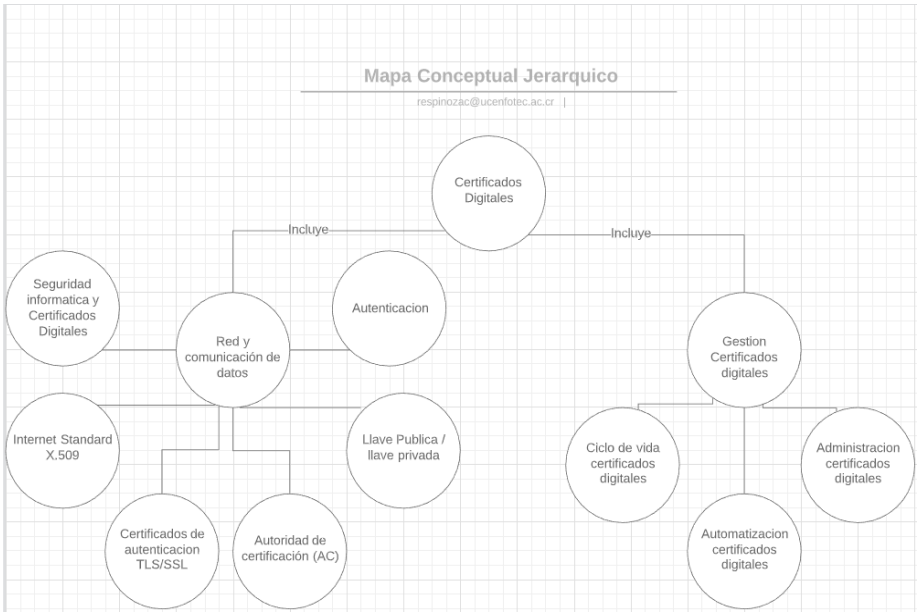


Fig. 3 Mapa conceptual Jerárquico conceptos

Fuente: Elaboración propia

2.1 Red y comunicación de datos

Una red básicamente consiste en la interconexión de dispositivos y equipos informáticos (computadoras y hardware de redes) utilizando medios de transmisión alámbricos o inalámbricos con el fin de transportar datos, compartir recursos, servicios e información para aplicaciones de cualquier tipo, es importante mencionar existen redes de área personal o pan se utiliza principalmente para conectar pequeña cantidad de dispositivos en una corta distancia, esta permite que la comunicación sea estable y rápida, también existen las redes tipo área local (LAN) conecta equipos en una área geográfica limitada por ejemplo oficina o edificios y por ultimo las redes de área amplia(WAN) que se caracteriza por una conexión de equipos informáticos ubicados geográficamente distanciados por ejemplo continentes diferentes.

La comunicación de datos es posible porque existe un medio de transmisión de la información digital(datos) entre el transmisor y receptor, existen medios alámbricos e inalámbricos. Cuando hablamos de medios alámbricos son cable UTP, cable

STP, cable FTP, fibra óptica, fibra monomodo y fibra multimodo. Medios inalámbricos tenemos: Microonda largo alcance (Wi-max), Microonda largo alcance (Wi-max) y Láser (FSO).

2.1.1 Seguridad informática y Certificados Digitales

En la actualidad las comunicaciones digitales se han convertido en nuestro diario vivir, en el principal medio para la economía mundial y de las relaciones sociales. La rápida evolución en la tecnología, ha permitido que los delitos informáticos se sofistiquen y diversifiquen, dentro de los principales tipos de ataques informáticos están: ARP Spoofing, man in the middle, IP spoofing, hijacking(secuestro de conexiones TCP), pharming, phishing, correo SPAM, software malicioso (Malware), efecto de un Worm, ataques de denegación de servicio (DoS),ataque DoS (SYN Flooding), ataque DDoS, botnet, vulnerabilidades a nivel de aplicación entre otros; es por ello que la seguridad informática es una prioridad para las empresas. En ese sentido certificado digital es una importante herramienta que garantiza la integridad de los datos, ya que ofrece mecanismos criptográficos que disminuye la posibilidad de un ciberataque.

2.1.2 Autenticación

La seguridad de los datos e información tiene como base cuatro pilares: la disponibilidad, la integridad, la confidencialidad y la autenticación. Para (comodo, 2024) autenticación se define como "The act of determining that a message has not been changed since leaving its point of origin. Authentication, secure authentication or secure SSL authentication of a user, is usually derived from something that the user understands, is or has. Many SSL Authentication Systems Which Provide SSL Internet Security and Online Payment System Security Are Now Shifting Toward Public Key Encryption". [El acto de determinar que un mensaje no ha sido

modificado desde que salió de su punto de origen. La autenticación, autenticación segura o autenticación SSL segura de un usuario, generalmente se deriva de algo que el usuario comprende, es o tiene. Muchos sistemas de autenticación SSL que brindan seguridad de Internet SSL y seguridad del sistema de pago en línea están cambiando ahora hacia el cifrado de clave pública.]

Las características más importantes de los certificados digitales son:

Autentificación. Para el receptor de un documento, la autentificación implica asegurar que los datos recibidos han sido enviados por quien declara ser poseedor de la identidad contenida en la firma digital. La autentificación de claves asimétricas permite que un mensaje cifrado con una clave privada sólo pueda haber sido enviado por el propietario de esta.

Confidencialidad. La confidencialidad implica asegurar que la información enviada no podrá ser interceptada por terceros. Para lograr la confidencialidad, el remitente (emisor) de un mensaje debe cifrarlo con la clave pública del destinatario (receptor), que puede obtenerse de su Certificado Digital. De esta forma el emisor se asegura que el mensaje sólo podrá ser descifrado con la clave privada del receptor, es decir, sólo podrá ser leído por el destinatario.

Integridad. La integridad de los documentos implica tanto para el remitente como para el destinatario asegurar que la información enviada no será modificada por terceros. Para garantizar la integridad, el remitente antes de enviar un mensaje aplica un algoritmo hash. De esta forma, al enviar un mensaje, el emisor envía el resultado del hashing cifrado junto con el mensaje original. Cuando el destinatario recibe el mensaje, recalcula el hashing del mensaje y lo compara si es igual al hashing recibido, para comprobar si el mensaje no ha sido modificado.

Privacidad. La privacidad de los mensajes implica que los datos sólo podrán ser leídos por el destinatario al estar cifrado.

No repudio. El no repudio implica para el receptor de un mensaje asegurar que el emisor no negará haber enviado la información recibida. Un mensaje "firmado" por su clave privada, una vez comprobada su integridad, impide al emisor el repudio del mensaje.

2.1.3 Llave Pública / llave privada

Los conceptos de llave publica y llave privada provienen del algoritmo de cifrado asimétrico, donde básicamente la llave pública se utiliza para encriptar y la llave privada para desencriptar, donde el emisor utiliza la llave pública del receptor para encriptar, y el receptor con su llave privada desencripta.

2.1.4 Internet Standard X.509

(appviewx, 2024) Define Internet Standard X.509 como "X.509 is a standard defining the format of public-key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the web. They are also used in offline applications, like electronic signatures. An X.509 (also called digital) certificate contains a public key and an identity (a hostname, or an organization, or an individual), and is either signed by a certificate authority or self-signed. When a certificate is signed by a trusted certificate authority, or validated by other means, someone holding that certificate can rely on the public key it contains to establish secure communications with another party, or validate documents digitally signed by the corresponding private key.

X.509 also defines certificate revocation lists, which are a means to distribute information about certificates that have been deemed invalid by a signing authority,

as well as a certification path validation algorithm, which allows for certificates to be signed by intermediate CA certificates, which are, in turn, signed by other certificates, eventually reaching a trust anchor" [X.509 es un estándar que define el formato de los certificados de clave pública. Los certificados X.509 se utilizan en muchos protocolos de Internet, incluido TLS / SSL, que es la base de HTTPS, el protocolo seguro para navegar por la web. También se utilizan en aplicaciones fuera de línea, como firmas electrónicas. Un certificado X.509 (también llamado digital) contiene una clave pública y una identidad (un nombre de host, una organización o un individuo) y está firmado por una autoridad certificadora o auto firmado. Cuando un certificado está firmado por una autoridad certificadora confiable o validado por otros medios, alguien que tenga ese certificado puede confiar en la clave pública que contiene para establecer comunicaciones seguras con otra parte o validar documentos firmados digitalmente por la clave privada correspondiente.

X.509 también define listas de revocación de certificados, que son un medio para distribuir información sobre certificados que una autoridad firmante ha considerado inválidos, así como un algoritmo de validación de ruta de certificación, que permite que los certificados sean firmados por certificados de CA intermedios, que son, a su vez, firmados por otros certificados, que finalmente alcanzan un ancla de confianza.] Es importante mencionar standard X.509 cuenta con las siguientes propiedades y características:

• El descriptor del certificado.

• La firma digital y un valor de firma.

• Versión. Contiene el número de versión del certificado codificado. Los valores aceptables son 1, 2 y 3.

• Número de serie. Es un entero asignado por la autoridad certificadora. Cada certificado emitido por una CA debe tener un número de serie único.

• Identificador del algoritmo de firmado. Identifica el algoritmo empleado para firmar el certificado. ACTA NOVA; Vol. 3, Nº3, diciembre 2006 Apuntes · 591

• Nombre del emisor. Identifica la CA que ha firmado y emitido el certificado.

• Periodo de validez. Indica el periodo de tiempo durante el cual el certificado es válido. Nombre del sujeto. Identifica el nombre del usuario para el que se emite el certificado.

• Nombre del sujeto. Indica el nombre del usuario para el cual se emite el certificado.

• Información de clave pública del sujeto. Información de la clave pública del usuario para el que se emite el certificado (nombre, algoritmo, etc.).

• Identificador único del emisor. Es un campo opcional que permite reutilizar nombres de emisor.

• Identificador único del sujeto. Es un campo opcional que permite reutilizar nombres de sujeto.

• Extensiones. Otros campos específicos de cada protocolo que están sujetos a sus propias regulaciones.

2.1.5 Certificados de autenticación TLS/SSL

Uno de los proveedores global de registro de nombres de dominio e infraestructura (certificados digitales) en internet más reconocido, define certificados SSL como "SSL stands for Secure Sockets Layer, a global standard security technology that enables encrypted communication between a web browser and a web server. It is utilized by millions1 of online businesses and individuals to decrease the risk of sensitive information (e.g., credit card numbers, usernames, passwords, emails, etc.)

from being stolen or tampered with by hackers and identity thieves. In essence, SSL allows for a private “conversation” just between the two intended parties.

To create this secure connection, an SSL certificate (also referred to as a “digital certificate”) is installed on a web server and serves two functions:

- It authenticates the identity of the website (this guarantees visitors that they’re not on a bogus site)
- It encrypts the data that’s being transmitted"(verisign, 2021) [SSL significa Secure Sockets Layer, una tecnología de seguridad estándar global que permite la comunicación cifrada entre un navegador web y un servidor web. Lo utilizan millones de empresas e individuos en línea para disminuir el riesgo de que la información confidencial (por ejemplo, números de tarjetas de crédito, nombres de usuario, contraseñas, correos electrónicos, etc.) sea robada o manipulada por piratas informáticos y ladrones de identidad. En esencia, SSL permite una "conversación" privada solo entre las dos partes previstas.

Para crear esta conexión segura, se instala un certificado SSL (también denominado "certificado digital") en un servidor web y tiene dos funciones:

- Autentica la identidad del sitio web (esto garantiza a los visitantes que no se encuentran en un sitio falso)
- Cifra los datos que se transmiten].

2.1.6 Autoridad de certificación (AC)

Una autoridad certificadora se puede entender como una entidad de confianza proveedora de servicios de certificados digital, dedicada a emitir nuevos certificados digitales y revocarlos cuando ya no son requeridos. Se caracteriza porque emplea la tecnología de criptografía de clave pública.

Según (comodo, 2024) una autoridad certificadora es "A third party organization which is used to confirm the relationship between a party to the https transaction and that party's public key. Certification authorities may be widely known and trusted institutions for internet based transactions, though where https is used on companies internal networks, an internal department within the company may fulfill this role". [Una organización de terceros que se utiliza para confirmar la relación entre una parte de la transacción https y la clave pública de esa parte. Las autoridades de certificación pueden ser instituciones ampliamente conocidas y confiables para transacciones basadas en Internet, aunque cuando se utiliza https en las redes internas de las empresas, un departamento interno dentro de la empresa puede cumplir esta función].

“Todas las Autoridades de Certificación deben mantener una base de datos de nombres distinguidos (ND) para usuarios o AC subordinadas y tomar las medidas para

asegurar que ninguna autoridad emita duplicados de ND. Las funciones más importantes que realizan las autoridades de certificación son:

• Registro de usuarios: tienen la responsabilidad de gestionar la información de identidad de los usuarios.

• Emisión de certificados: deben generar los certificados que enlacen a un usuario con una clave pública.

• Administración de certificados: además de registrar deben controlar atributos de los certificados para tomar decisiones de revocación, renovación y suspensión.

• Servicio de consulta: deben ofrecer servicios a los usuarios para facilitar el seguimiento sobre el estado de los certificados.

• Administración de las firmas: deben ofrecer mecanismos para la generación de claves usando algoritmos de cifrado de mensajes.” (Herrera, J., & Fernández, D. ,2006)

En Costa Rica el BCCR es la autoridad certificadora acreditada para emitir certificados digitales, la entrega de los certificados digitales se realiza por medio instituciones financieras nacionales previamente autorizadas por esta institución como Oficina de Registro. A nivel mundial algunas de las autoridades certificadoras más importantes son:

- Symantec
- GeoTrust
- Comodo
- DigiCert
- Thawte
- GoDaddy
- Network Solutions
- RapidSSLonline
- SSL.com
- Entrust Datacard
- Venafi

2.2 Gestión Certificados digitales

El proceso de certificación digital (Herrera, J., & Fernández, D. ,2006) lo describe de la siguiente manera:”

a) Generación de la clave. La entidad que solicita la certificación (el solicitante, no la entidad emisora) para generar pares de claves públicas/privadas y algoritmos de cifrado. La clave pública puede ser la misma que tiene la

autoridad de certificación.

b) Encapsulado de las firmas. El solicitante empaqueta la información de identidad y los atributos necesarios para que la autoridad de certificación emita el certificado.

c) Envío de las claves públicas y la información. El solicitante envía las dos claves y la información a la autoridad de certificación.

d) Comprobación de la información. La autoridad de certificación utiliza la información enviada por el solicitante para tomar la decisión de emitir el certificado.

e) Creación del certificado. La autoridad de certificación crea un documento digital que contiene la información atribuida a la entidad solicitante y lo firma con su clave privada.

f) Envío y publicación del certificado. La autoridad de certificación puede enviar el certificado al solicitante o publicarlo si resulta más apropiado.

g) Instalación del certificado. El procedimiento de instalación de un certificado varía de acuerdo con el ambiente del sistema”

Para (ADMWARE, s.f.) las características principales de la gestión de certificados digitales son:”

- Se instala el certificado en el servidor. No se instala en los equipos.
- Las firmas digitales son llevadas a cabo por el servidor que es quien tiene el certificado digital instalado.
- La clave privada del certificado nunca sale del servidor.
- Auditoría centralizada de las operaciones.
- Permite avisar de cuando se pretende utilizar el certificado para un proceso de firma.

- Otorga la posibilidad asignar roles a los usuarios. Permite definir el uso de un certificado en base a usuario/grupo del directorio, hora y fecha, IP origen, programa que invoca, URL de acceso.
- Notificación al propietario de vencimiento de certificado.
- Portal web para gestionar los certificados.
- Posibilidad de establecer arquitectura de alta disponibilidad para entornos con un requerimiento de continuidad.
- Herramienta para escanear toda la red en busca de certificados instalados en puestos.
- Agente con capacidad para ser desplegado casi en cualquier entorno empresarial.
- Cliente PKCS#11 para integración con servidores J2EE que realizan firma digital.
- Integración nativa con HSMs de red de Safenet y Thales. Soporte para integración con otros HSM de red.
- Webservices de firma digital PDF, XMLDsig, PKCS#7.
- Integración nativa con HSMs de red de Safenet y Thales. Soporte para integración con otros HSM de red.
- Flujos de trabajo para la firma digital.
- Aplicación portafirmas para estación de trabajo y dispositivos móviles.
- Listas blancas de navegación web para direcciones URL.
- Uso de los certificados mediante ACLs de control para páginas web y programas.”.

2.2.1 Ciclo de vida certificados digitales

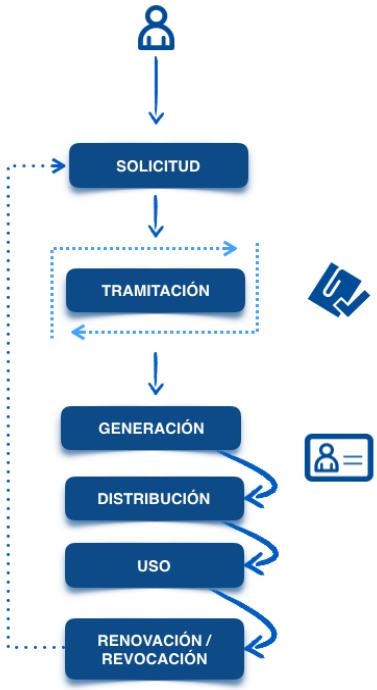


Fig. 4 Ciclo de vida certificados digitales.

Fuente: Viafirma RA (s.f.).

Solicitud: Acá inicia el ciclo, para asegurar un sitio web se debe adquirir un certificado digital de tipo SSL/TLS, se genera una solicitud de certificado a la AC para el servidor web que desea asegurar.

Tramitación: En esta etapa la entidad certificadora recibe la solicitud y la procesa.

Generación: Cuando la tramitación se completa, el sistema genera el nuevo certificado para su instalación.

Distribución: El solicitante puede bajar el nuevo certificado para posteriormente instalarlo en el servidor web deseado.

Uso: Un vez distribuido el certificado digital, el titular o solicitante pasa a ser el dueño y responsable de este, se instala y entra en funcionamiento en el servidor.

Renovación/Revocación: Todos los certificados desde que son creados cuentan con una fecha de caducidad. Llegado a este momento el dueño o titular del

certificado debe decidir si renovar su certificado, generando una nueva solicitud, o revocar y eliminar el certificado del servidor web.

2.2.2 Administración certificados digitales

Cuando se habla de administración del ciclo de vida de los certificados digitales Enterprise, se refiere a una plataforma informática diseñada para que un profesional de TI desde una consola pueda administrar todos los certificados Enterprise. La solución permite a los administradores de TI encontrar certificados, alerta al vencimiento certificados, recuperar certificados eliminados e implementar certificados en nuevos servidores, garantizar comunicaciones cifradas y las transacciones se mantienen seguras.

2.2.3 Automatización certificados digitales

Con respecto a la automatización de certificados digitales, la empresa AppViewx define "is defined as the ability of a security system to be able to rapidly switch between algorithms, cryptographic primitives, and other encryption mechanisms without the rest of the system’s infrastructure being significantly affected by these changes.

In other words, it is the ability of an organization to possess complete control over its cryptographic mechanisms and processes, allowing them to make accurate alterations to them without involving intense manual effort. This is an important ability to have, since the principle of accelerating change guarantees that developments in computing power and security will continue to occur at a heightened pace, rendering existing crypto-systems obsolete in a few years unless they are upgraded to the latest version – since threats continue to evolve along with them. Furthermore, with the phenomenon of digital transformation resulting in cryptography being built into virtually every communication system in the world, cryptography cannot remain

isolated from other critical systems – making it imperative for administrative teams to have visibility into their crypto-systems in order to effect rapid change when deemed necessary. The looming threat of quantum computing is another compelling reason for organizations to consider becoming crypto-agile.

A robust, cryptographically agile information system will prove to be invaluable to organizations in the long term, and will play a critical role in preventing security breaches, making SecOps teams more efficient, and eliminating monetary losses that may be expended as consulting fees, fines, or remediation" (AppViewX, 2024)[se define como la capacidad de un sistema de seguridad para poder cambiar rápidamente entre algoritmos, primitivas criptográficas y otros mecanismos de cifrado sin que el resto de la infraestructura del sistema se vea afectado significativamente por estos cambios.

En otras palabras, es la capacidad de una organización de poseer un control completo sobre sus mecanismos y procesos criptográficos, permitiéndoles realizar alteraciones precisas en ellos sin involucrar un esfuerzo manual intenso. Esta es una habilidad importante que se debe tener, ya que el principio de cambio acelerado garantiza que los desarrollos en la potencia informática y la seguridad continuarán ocurriendo a un ritmo acelerado, haciendo que los sistemas criptográficos existentes se vuelvan obsoletos en unos pocos años a menos que se actualicen a la última versión. ya que las amenazas continúan evolucionando junto con ellas. Además, con el fenómeno de la transformación digital que da como resultado que la criptografía se integre en prácticamente todos los sistemas de comunicación del mundo, la criptografía no puede permanecer aislada de otros sistemas críticos, por lo que es imperativo que los equipos administrativos tengan visibilidad de sus cripto-sistemas para lograr un efecto rápido. cambiar cuando se considere necesario. La

inminente amenaza de la computación cuántica es otra razón convincente para que las organizaciones consideren convertirse en cripto-ágiles.

Un sistema de información robusto y criptográficamente ágil resultará invaluable para las organizaciones a largo plazo y desempeñará un papel fundamental en la prevención de violaciones de seguridad, haciendo que los equipos de SecOps sean más eficientes y eliminando las pérdidas monetarias que se pueden gastar como honorarios de consultoría, multas, o costos de remediación]

Capítulo 3. Marco Metodológico

3.1 Tipo de Investigación

Tal como lo explica Hernández, Fernández & Baptista (2010) la investigación científica es

> en esencia, como cualquier tipo de investigación, sólo que más rigurosa, organizada y se lleva a cabo cuidadosamente. Como siempre señaló Fred N. Kerlinger: es sistemática, empírica y crítica. Esto se aplica tanto a estudios cuantitativos, cualitativos o mixtos. Que sea “sistemática” implica que hay una disciplina para realizar la investigación científica y que no se dejan los hechos a la casualidad. Que sea “empírica” denota que se recolectan y analizan datos. Que sea “crítica” quiere decir que se evalúa y mejora de manera constante. Puede ser más o menos controlada, más o menos flexible o abierta, más o menos estructurada, en particular bajo el enfoque cualitativo, pero nunca caótica y sin método.
>
> Tal clase de investigación cumple dos propósitos fundamentales: a) producir conocimiento y teorías (investigación básica) y b) resolver problemas (investigación aplicada). Gracias a estos dos tipos de investigación la

humanidad ha evolucionado. La investigación es la herramienta para conocer lo que nos rodea y su carácter es universal (p.27).

En función de los objetivos definidos en la presente investigación, se puede determinar no se va a generar conocimiento nuevo, ya que sabemos que es lo que perseguimos y procura generar conocimiento en base a estudios previos con respecto a mejores prácticas y técnicas existentes para ciclo de vida de los certificados digitales que permitan contribuir a solucionar el problema. Es por esto se considera como una investigación de tipo aplicada y evaluativa.

3.2 Alcance Investigativo

Según la naturaleza y el contexto de la presente investigación se concluye que el alcance a utilizar es:

3.2.1 Explicativo: De acuerdo con la definición de Muñoz (2015) sobre investigación explicativa: “este tipo de investigación son más profundas; sin duda, para alcanzar estos niveles se debe contar con estudios, con información más abundante y, en consecuencia, es posible centrar la atención en encontrar los orígenes, las causas o los factores determinantes del hecho o fenómeno investigado” (p.85). Hernández, Fernández, & Baptista, (2006) resume investigación explicativo como:” Determinan las causas de los fenómenos. Generan un sentido de entendimiento. Combinar sus elementos en un estudio”. Se considera que es un estudio de alcance explicativo ya que actualmente existe conocimiento del tema, y busca entender y establecer la causa de los fallos.

3.2.2 Descriptivo: Hernández, Fernández, & Baptista, (2006) explica que: “los estudios descriptivos son útiles para mostrar con precisión los ángulos o dimensiones de un fenómeno, suceso, comunidad, contexto o situación.”. La presente investigación se clasifica como descriptivo debido a que existe literatura

previa sobre el tema en estudio, esta literatura nos ayuda como base y para fundamentar el estudio. Específicamente para el presente proyecto vamos a medir herramientas actuales en el mercado, recolectar datos, y analizar cómo se manifiesta el ciclo de vida de certificados digitales.

3.3 Enfoque

Bajo la perspectiva de autores como Chavarría (2011) donde indica que los enfoques cualitativos y cuantitativos no pueden existir de manera separada y que, más aún, no tiene sentido hablar de enfoques mixtos pues estos intentan mezclar de manera artificiosa cosas que nunca han estado desligadas, se propone un abordaje de tipo alternativo para la presente investigación. Dicho enfoque consiste en 3 dimensiones:

3.3.1 Epistemológica

Tal como nos lo explica Naranjo-Zeledón (2020) la dimensión epistemológica es la postura del investigador con respecto al tema u objeto de estudio, existen 2 posibles posturas como observador o involucrado con el objeto de estudio. En investigaciones de tipo puro o evaluativo, normalmente el investigador asume una postura de observador y relator de lo acontecido. En las de tipo aplicado, por el contrario, es necesario interactuar e involucrarse directamente con lo estudiado.

Para el presente proyecto de investigación, se toma una postura de tipo aplicado ya que el investigador estará activamente involucrado en toda la investigación, documentación, implementaciones, pruebas, análisis y propuestas.

3.3.2 Ontológico

Definición y explicación dada por (Naranjo-Zeledón, 2020) en informática se entiende por ontología como un conjunto de términos básicos y relaciones entre ellos. La representación ontológica del objeto de estudio se hace explícita entonces con una figura que deja claros los elementos y relaciones a estudiarse. Debe ser explícita debido a que es necesario especificar de forma consciente todos los conceptos relevantes que conforman la ontología. Por otra parte, debe ser presentarse de manera formal por medio de un lenguaje de representación formalizado. Por último, ha de ser compartida, dado que será presentada a la comunidad encargada de evaluarla y usarla.

Partiendo de la explicación anterior el presente proyecto es ontológico ya que existen múltiples estudios y propuestas previas sobre el tema de automatización del ciclo de vida de los certificados digitales, demostrando que lo que estamos estudiando ya existe.

3.3.3 Axiológico

Para (Naranjo-Zeledón, 2020) la dimensión axiología se encarga de estudiar los valores, clasifica que son buenas y qué tan buenas son. La importancia de la axiología es que permite formalizar escalas de valores para no utilizar conceptos cuya definición o medición de su valor intrínseco resulta muy vaga, como por ejemplo robustez, amigabilidad o eficiencia. Esto resulta sumamente útil para lograr un cometido básico de los objetivos y es que estos sean medibles. También resulta muy apropiado en investigaciones de tipo aplicado o evaluativo. Para efectos de este trabajo, la tabla #15 se muestra las variables que utilizamos para evaluar las propuestas seleccionadas.

Tabla 15 *Criterio de evaluación*

Categorías	Peso %	Comentarios / Definición
Escalabilidad	10	Es la capacidad de adaptación de un sistema con respecto al rendimiento de este a medida que aumentan de forma significativa el número de usuarios.
Compatibilidad	10	Es la capacidad de soportar los diferente tipos de sistema operative, base de datos y navegadores web.
Integraciones	10	¿La solución ofrece integraciones con su tecnología actual (ITSM, SIEM, HSM, CA, CI/CD, etc.)? ¿Son las integraciones plug-and-play y listas para usar?
Arquitectura de implementación	10	¿Cuál es la base subyacente del producto? ¿Está construido sobre una plataforma de microservicios moderna y expandible? ¿La automatización es el núcleo de la solución? ¿Es un producto SaaS totalmente funcional?
Facilidad de implementación, administración y mantenimiento.	10	Asegurarse que las operaciones de la herramienta requieran la menor cantidad de recursos necesarios para cumplir con los requisitos.
APIs/Automatización	10	¿Puede personalizar la solución para adaptarla a sus requisitos específicos? ¿Puede crear fácilmente sus propios flujos

Categorías	Peso %	Comentarios / Definición
		de trabajo de automatización personalizados para sus casos de uso únicos? Como, por ejemplo: Renovación de los certificados digitales. Que cuente con funciones de automatización, como renovar y eliminar automáticamente ¿La solución ofrece APIs para integraciones más personalizadas? Fácil integración entre otros sistemas.
Reportes	10	Debe contar con flexible módulo de reporteo.
Industria	5	La industria es la actividad económica a la que se dedica la compañía. Se evaluará cuales son los principales consumidores de la solución.
Innovación	5	Se tomará en cuenta si la solución incluye nuevas ideas, métodos, productos, servicios o funcionalidades que tengan un impacto positivo y beneficioso.
Análisis y conclusiones	20	En este punto se evaluará si la herramienta cuenta con las funcionalidades requeridas para solucionar los problemas expuestos en este trabajo de investigación.

Fuente: Elaboración propia

3.4 Diseño

El diseño de la investigación en estudio es de tipo evaluativa ya que este evalúa programas, sugiere mejora continua, utiliza estándares, propone nuevos sistemas de información y capacitación.

Se realizará un proceso de análisis para medir productos, servicios y procesos de una empresa frente a la otra. Para ello, utilizamos como base de comparación empresas líderes en sus respectivos sectores.

Para lograr los objetivos de la investigación se desarrollarán las siguientes etapas:

- Definir qué competidores se analizarán: mínimo 2 empresas, las cuales deben operar en segmentos de negocio similares.
- Establecer los indicadores que se analizarán: comparar aspectos específicos en función de las métricas definidas.
- Reunir datos: realizar estudios de mercado sobre el competidor.
- Comparar los datos: análisis exhaustiva que permita evaluar el rendimiento de sus aplicaciones en un entorno altamente competitivo.
- Identificar los aspectos más destacados: a partir de la comparación efectuada, será posible comprender en qué destaca el competidor y sus limitaciones.
- Análisis final y conclusiones.

3.5 Población y Muestreo

Se define población como una colección finita o infinita de elementos en consideración, la población es el punto de partida para recolectar datos. Mientras que muestra es una cantidad pequeña que se considera representativa del total y es utilizada para estudios (Oxford Dictionaries, s.f.).

Para efectos de esta investigación al tener enfoque alternativo no es necesario consultar a toda la población u obtener datos estadísticos. Se elige un muestreo no probabilístico por conveniencia, pues se trabaja con grupos o departamentos de TI específicos (Windows IIS y certificados SSL/TLS únicamente) que serán elegidos por el investigador.

Con el fin de contar con suficientes datos para el análisis y dar validez a los hallazgos se seleccionarán con cierta intencionalidad y afinidad 4 grupos de TI diferentes, y se entrevistara a los representantes expertos en el ciclo de vida de los certificados digitales.

Es importante aclarar por razones de políticas internas de Intel con respecto al manejo de la seguridad de la información personal y conciencia de la privacidad de los datos, es que no se van a mencionar los nombres de las personas entrevistadas, sin embargo, si se va a indicar las organizaciones respectivas de las personas expertas entrevistadas. En la presente tabla se detalla esta información:

Tabla 16 *Expertos entrevistados*

Identificador	Entrevistado	Organización
PE1	Persona entrevistada #1	PEIT QUALITY& STRESS LABS
PE2	Persona entrevistada #2	IT EOG EPSE Data & PLTF
PE3	Persona entrevistada #3	IT EOG EPSE Data & PLTF
PE4	Persona entrevistada #4	Supply Chain Source & Procure
PE5	Persona entrevistada #5	IT EOG ICC Ctrl Escalation Mgr
PE6	Persona entrevistada #6	IT EOG ICC Ctrl Escalation Mgr

Fuente: Elaboración propia

3.6 Instrumentos de Recolección de Datos

Para (Merriam-Webster, s.f.) define la recolección como el acto o proceso de obtener cosas (datos) de diferentes lugares, unirlas para estudio y así alcanzar los objetivos propuestos.

Con el fin de contar con un panorama más claro de la infraestructura tecnológica de Intel y sus oportunidades de mejora o amenazas, se creó la encuesta de la figura #5, la cual se compartirá con las organizaciones de TI previamente seleccionadas y los responsables técnicos de las aplicaciones, adicionalmente se realizará entrevistas a personas claves expertas en el tema y se aplicará la técnica de observación directa en grupos focales.

La encuesta se creó en la plataforma survey monkey donde se van a presentar 17 preguntas cerradas y 3 preguntas abiertas referidas al manejo de certificados digitales que permitirán recolectar información necesaria para el desarrollo del diagnóstico. Las personas entrevistadas podrían ser de cualquier país donde Intel tiene operaciones, es por esta razón que fue elaborada en el idioma inglés.

1. Please, enter your employeeID.

2. Please, enter the application name:

3. Application number:

4. Operating System:

- ◯ Windows
- ◯ Linux

Other (please specify)

5. Web Server:

- ◯ IIS
- ◯ Apache
- ◯ Other (please specify)

6. Facing: *

- ○ Internal only
- ○ External only
- ○ Both (Internal and External)

7. Geo Location: *

- ☐ AMR
- ☐ GER
- ☐ GAR

8. Customer base (approx. # of users): *

Enter your answer

9. Network Type: *

- ○ GPB
- ○ SIZ (Secure Internal Zone)
- ○ HTZ (High Trust Zone)
- ○ Azure (Microsoft)
- ◉ AWS (Amazon)
- ○ GCP (Google Cloud Platform)
- ○ Other

10. The application host certificates on load balancer? *

- ○ Yes
- ○ No

11. How many certificates manage your platform ?

12. How do you manage certificates expiration date?

13. How long does it take to complete a manual certificate renewal?

14. Main challenge associated with manually managing CA's:

- ◯ Single Point of failure.
- ◯ Lack technical documentation.
- ◯ Knowledge transfer.
- ◯ Human errors while renewal/revoke certificates.
- ◯ limited certificate management capabilities.
- ◯ keep track of issued certificates and maintain compliance.
- ◯ Lack certificate renewal automation.
- ◯ Mismanaged SSL/TLS certificates
- ◯ Other (please specify)

15. Explain why?

16. How did you solved this problem?

17. How long did it take you to resolve the problem?

18. To solve this problem do you require additional help?

- ◯ Yes
- ◯ No
- ◯ If yes, please specify:

19. What are the security pillars most affected when managing certificates manually? 1 Most - 7 Less

	1	2	3	4	5	6	7
Availability	☐	☐	☐	☐	☐	☐	☐
Integrity	☐	☐	☐	☐	☐	☐	☐
Confidentiality	☐	☐	☐	☐	☐	☐	☐
Authenticity	☐	☐	☐	☐	☐	☐	☐
Non-repudiation	☐	☐	☐	☐	☐	☐	☐
Safety	☐	☐	☐	☐	☐	☐	☐
Privacy	☐	☐	☐	☐	☐	☐	☐

20. Describe how manual renewal of certificate affect security pillars?

Fig. 5 Encuesta a toda la población de dueños de aplicaciones para la compañía.
Fuente: Elaboración propia

3.7 Técnicas de Análisis de Información

Para este propósito, se utilizó la técnica espina de pescado Ishikawa, ya que nos permite representar de manera gráfica la causa-efecto. El diagrama de espina de pescado nos permite recolectar todos los datos de la encuesta y le dan uso efectivo para la investigación. Se lista todas las variables que forman parte del ciclo de vida del certificado digital para luego poder realizar el analices respectivo de las posibles causas del problema.

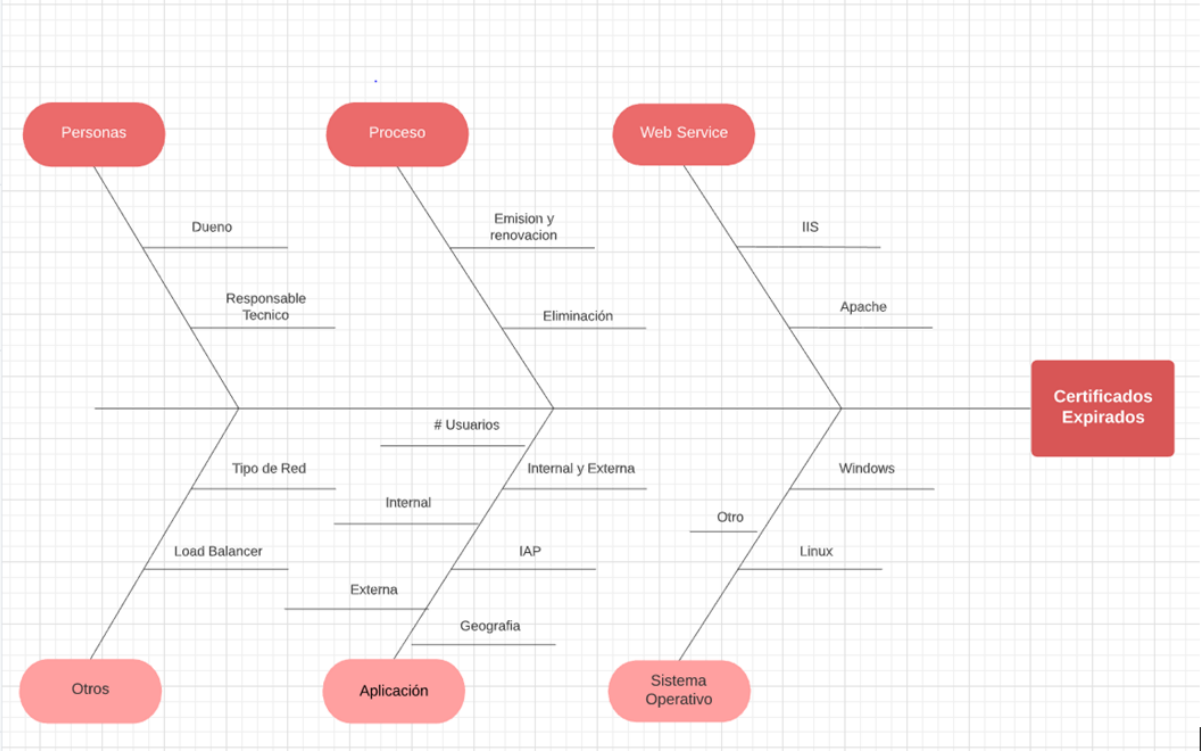


Fig. 6 Diagrama de espina de pescado.

Fuente: Elaboración propia

3.8 Estrategia de Desarrollo de la Propuesta

La etapa 1 consiste en la investigación de las mejores prácticas en el mercado sobre gestión y manejo del ciclo de vida de los certificados digitales Enterprise. A través de un benchmarking se pretende realizar estudios exhaustivos de diferentes softwares gestores de certificados digitales, que permitan

la emisión de certificados a través de una plataforma, que garantice la emisión más ágiles y controlando todo el ciclo de vida de los certificados.

Para la etapa 2 se planea realizar un análisis profundo con los principales software del mercado en el manejo de certificados digitales corporativos, como por ejemplo Venafi, Appviewx, Letsencrypt.org y Sectigo por mencionar algunos.

Y por último en la etapa 3, se pretende realizar una evaluación y análisis de los principales resultados que generados en la etapa 2, con la finalidad de hacer una propuesta final de una herramienta empresarial que sea rentable, se adapte a las necesidades de la empresa y se alinee a la arquitectura de Intel.

Capítulo 4. Análisis del Diagnóstico

El instrumento de recolección de datos del apartado 3.6 fue de mucho valor, ya que a través de este se pudo tener acceso a información relevante con respecto a la situación actual en el manejo de la gestión de los certificados digitales, así como de las opiniones de las personas expertas en el área.

4.1 Aplicación de entrevista a expertos

Como parte del análisis, se realizó una breve investigación y selección de las personas técnicas idóneas para la aplicación de la entrevista, como resultado de este filtro se obtuvieron seis ingenieros de cuatro grupos diferentes que se detallan en la tabla #16.

Es importante destacar que para efectos de este apartado se hizo una selección de las preguntas más relevantes para esta investigación, ya que algunas de las preguntas del cuestionario cuentan con información de carácter confidencial para la empresa.

Luego de aplicar el instrumento a las personas identificadas, se lograron obtener los siguientes resultados.

4.1.1 Resultados de entrevista a representante experto del equipo PEIT QUALITY& STRESS LABS

Para esta organización se logró identificar únicamente una persona experta a quien se le asigno el identificador PE1, sus respuestas se presentan a continuación en la tabla #17.

Tabla 17 *Respuestas de PE1*

Pregunta	Respuesta
Sistema Operativo	PE1: R/ Microsoft Windows Server 2019
Webservice	PE1: R/ IIS
Tipo de aplicación (externa o interna)	PE1: R/ Interna
Tipo de red	PE1: R/ High Trust Zone
¿Cómo controla la fecha de vencimiento de los certificados digitales?	PE1: R/ La renovación es un proceso manual que se realiza anualmente.
¿Cuánto tiempo toma completar la renovación de certificado digitales manualmente?	PE1: R/ Tomaba alrededor de 30 minutos
¿Cuántos certificados TLS/SSL administra su organización/departamento?	PE1: R/ 15
¿Cuál es el principal reto asociado al manejo manual de renovación de certificados digitales?	PE1: R/ Errores humanos al renovar/revocar certificados.
¿Explique por qué?	PE1: R/ Situación: El certificado se había actualizado, pero en el CI/CD estaba referenciado a la versión anterior y esto provocó que el certificado vencido se configurara en producción.
¿Cómo resolvió este problema?	PE1: R/ Instalando manualmente en producción el certificado manualmente y actualizando el CI/CD
¿Cuánto tiempo te llevó resolver el problema?	PE1: R/ 1 hora

¿Para solucionar este problema necesitas ayuda adicional? En caso afirmativo, especifique	PE1: R/ No
¿Cuáles son los pilares de seguridad más afectados al gestionar los certificados manualmente? 1 más - 7 menos	Disponibilidad. (3) Integridad. (2) Confidencialidad. (1) Autenticidad. (6) No repudio. (7) Seguridad. (4) Privacidad. (5)
Describa con amplitud cómo la renovación manual del certificado afecta los pilares de seguridad.	La gestión manual de la renovación de certificados puede provocar que se dé el vencimientos de certificados, lo que provoca interrupciones del servicio o que se presenten violaciones de seguridad, afectando la disponibilidad, integridad, seguridad de los datos y demás pilares.

Fuente: Elaboración propia

4.1.2 Resultado de entrevista a representantes expertos del equipo IT EOG EPSE Data & PLTF

Para esta organización IT EOG EPSE Data & PLTF se logró identificar dos expertos en el área de certificados digitales, a quienes se les asignó el identificador PE2 y PE3, sus respuestas se presentan a continuación en la tabla #18.

Tabla 18 *Respuestas de PE2 y PE3*

Pregunta	Respuesta
Operating System	PE2: R/ Microsoft Windows Server/ Linux SuSE Enterprise Server
	PE3: R/ Microsoft Windows Server/ Linux SuSE Enterprise Server
WebServer	PE2: R/ IIS
	PE3: R/ IIS
Facing	PE2: R/ Internal
	PE3: R/ Internal
Network Type:	PE2: R/ High Trust Zone
	PE3: R/ High Trust Zone

¿How do you manage certificates expiration date?	PE2: R/ Manual Process. [Proceso Manual]
	PE3: R/ We will receive notification that a particular certificate will expires within xx days. [Recibimos una notificación de que un certificado en particular caducará dentro de xx días.]
¿ How long does it take to complete a manual certificate renewal?	PE2: R/ For 1 machine around 25 mins. [Para 1 máquina unos 25 minutos.]
	PE3: R/ Averagely, it takes within 30mins. Some will need to be done during maintenance downtime, i.e. the high wire/load balancing servers. [En promedio, demora 30 minutos. Algunos servidores se hacen durante los trabajos de mantenimiento planificados, por ejemplo: los servidores de balanceador de carga]
¿How many certificates manage your platform?	PE2: R/ 21
	PE3: R/ roughly around 45. [aproximadamente alrededor de 45]
Main challenge associated with manually managing CA's:	PE2: R/ Lack technical documentation and Human errors while renewal/revoke certificates. [Falta de documentación técnica y errores humanos al renovar/revocar certificados.]
	PE3: R/ Single point of failure, creating dependency on one expert/person. [Punto único de falla, creando dependencia de un experto/persona]
¿ Explain why?	PE2: R/Steps can be confusing and lack of confidence in performing the certificate renewal for new implementor. [Los pasos pueden resultar confusos y generar falta de confianza al realizar la renovación del certificado para un nuevo implementador].
	PE3: R/ The only person in charge of this process, was retired. she Left the organization, and no one was familiar how to do it. [El único responsable de este proceso, fue jubilado. Ella dejó la organización y nadie sabía cómo

	hacerlo].
¿ How did you solve this problem?	PE2: R/ Documenting with more details and screen shots. [Documentar con más detalles y capturas de pantalla].
	PE3: R/ The organization had to reach out the expert even after worked for Intel, also request additional help from PKI team. [La organización tuvo que comunicarse con el experto incluso después de trabajar para Intel y también solicitar ayuda adicional del equipo de PKI.]
¿ How long did it take you to resolve the problem?	PE2: R/ 3 working days' worth of hours spent in discussing and documenting. [3 días hábiles de horas dedicadas a discutir y documentar].
	PE3: R/ Is an ongoing effort learn by our self without proper pass down or training. [Es un esfuerzo continuo de aprender por nosotros mismos sin una transmisión o capacitación adecuada.]
To solve this problem do you require additional help? If yes, please specify	PE2: R/ Yes. Discussion and seeking verification/confirmation from with peers. [Sí. Discusiónes y búsqueda de verificación/confirmación con compañeros].
	PE3: R/ Correct the team needed to contact PKI department, and as well our ex-teammate. [Correcto, el equipo necesito contactar al departamento de PKI y también a nuestro ex compañero de equipo].
¿ What are the security pillars most affected when managing certificates manually? 1 Most - 7 Less	PE2: R/ Availability. (1) Integrity. (3) Confidentiality. (4) Authenticity. (4) Non-repudiation. (4) Safety. (3) Privacy. (3)

	PE3: R/ Availability. (5) Integrity. (2) Confidentiality. (6) Authenticity. (1) Non-repudiation. (7) Safety. (3) Privacy. (4)
¿ Describe how manual renewal of certificate affect security pillars?	PE2: R/ In my opinion, renewal would mostly impact the productivity of the implementor as it would take more time to perform manual tasks. Concern on security pillars will come in when there is risk of human error of downloading the wrong file to the wrong server. If the wrong file is in the server, it would impact the application that is hosted by the server. [En mi opinión, la renovación afectaría principalmente a la productividad del implementador, ya que toma mucho tiempo realizar tareas manuales. La preocupación por los pilares de seguridad surgirá cuando exista el riesgo de que se produzca un error humano al descargar el archivo incorrecto en el servidor equivocado. Si el archivo incorrecto está en el servidor, afectaría la aplicación alojada en el servidor].
	PE3: R/ Transport Layer Security (TLS) is a cryptographic protocol for providing privacy and data security for communications over the computer network. TLS was derived from security protocol called Secure Socket Layer (SSL) and it ensures that no third party may eavesdrop or tampers the message. To accomplish security, integrity and authenticity TLS makes use of certificates to communicate between 2 applications. [Transport Layer Security (TLS) es un protocolo criptográfico para proporcionar privacidad y seguridad de datos para las comunicaciones a través de la red informática. TLS se derivó del

	protocolo de seguridad llamado Secure Socket Layer (SSL) y garantiza que ningún tercero pueda espiar o alterar el mensaje. Para lograr seguridad, integridad y autenticidad, TLS utiliza certificados para comunicarse entre dos aplicaciones].

Fuente: Elaboración propia

4.1.3 Resultados de entrevista a representante experto del equipo Supply Chain Source & Procure

Para esta organización se logró identificar únicamente una persona experta a quien se le asigno el identificador PE4, sus respuestas se presentan a continuación en la tabla #19.

Tabla 19 *Respuestas de PE4*

Pregunta	Respuesta
Sistema Operativo	PE4: R/ Microsoft Windows Server 2019
Webservice	PE4: R/ IIS/Apache Tomcat
Tipo de aplicación (externa o interna)	PE4: R/ Interna
Tipo de red	PE4: R/ High Trust Zone
¿Cómo controla la fecha de vencimiento de los certificados digitales?	PE4: R/ Se realizan reuniones mensuales para revisar su fecha de vencimiento. También se reciben notificaciones cuando un certificado está próximo a vencer.
¿Cuánto tiempo toma completar la renovación de certificado digitales manualmente?	PE4: R/ Aproximadamente 3 horas
¿Cuántos certificados TLS/SSL administra su organización/departamento?	PE4: R/ Siete certificados
¿Cuál es el principal reto asociado al manejo manual de renovación de certificados digitales?	PE4: R/ Mantener actualizados los certificados digitales emitidos.
¿Explique por qué?	PE4: R/ Se tiene un gran inventario de certificados y se debe estar atento a cuando se vencen. Se han dado

	ocasiones en que debido a la no renovación de certificados una aplicación deja de funcionar.
¿Cómo resolvió este problema?	PE4: R/ Con revisiones periódicas
¿Cuánto tiempo te llevó resolver el problema?	PE4: R/ Dos meses
¿Para solucionar este problema necesitas ayuda adicional? En caso afirmativo, especifique	PE4: R/ No
¿Cuáles son los pilares de seguridad más afectados al gestionar los certificados manualmente? 1 más - 7 menos	PE4: R/ Disponibilidad. (1) Integridad. (5) Confidencialidad. (4) Autenticidad. (6) No repudio. (7) Seguridad. (2) Privacidad. (3)
Describa con amplitud cómo la renovación manual del certificado afecta los pilares de seguridad.	PE4: R/ Los sitios pueden estar no disponibles a los usuarios pues si no se renuevan a tiempo los certificados bloquean el acceso. Al mismo tiempo la información que se ingresa en las diferentes aplicaciones podría verse comprometida.

Fuente: Elaboración propia

4.1.4 Resultado de entrevista a representantes expertos del equipo IT EOG ICC Ctrl Escalation Mgr

Para esta organización IT EOG ICC Ctrl Escalation Mgr se logró identificar dos expertos en el área de certificados digitales, a quienes se les asignó el identificador PE5 y PE6, sus respectivas respuestas se presentan a continuación en la tabla #20.

Tabla 20 *Respuestas de PE5 y PE6*

Pregunta	Respuesta
Sistema Operativo	PE5: R/ Microsoft Windows Server 2019
	PE6: R/ Windows
Webservice	PE5: R/ IIS / Apache Tomcat
	PE6: R/ IIS / Apache Tomcat
Tipo de aplicación (externa o interna)	PE5: R/ Interna/Externa
	PE6: R/ Interna/Externa
Tipo de red	PE5: R/ HTZ
	PE6: R/ HTZ
¿Cómo controla la fecha de vencimiento de los certificados digitales?	PE5: R/ Manualmente con hoja de Excel y notificación automática de la plataforma en uso.
	PE6: R/ De manera manual se lleva el control.
¿Cuánto tiempo toma completar la renovación de certificado digitales manualmente?	PE5: R/ Máximo 30 minutos si no hay fallos humanos
	PE6: R/ 30 minutos sin errores
¿Cuántos certificados TLS/SSL administra su organización/departamento?	PE5: R/ 25
	PE6: R/ 25
¿Cuál es el principal reto asociado al manejo manual de renovación de certificados digitales?	PE5: R/ Único punto de fallo
	PE6: R/ Errores humanos al renovar/revocar certificados.
¿Explique por qué?	PE5: R/ La renovación manual de certificados expone a la compañía a punto de fallo único, que es la intervención humana manual. Para la renovación de un único o de pocos certificados, se cuentan con el riesgo principal de que la persona encargada olvide renovarlos. Pero, en infraestructuras más grandes y complicadas, se presenta el reto de renovar muchos certificados que pueden necesitar de equipos muy grandes y de mucho tiempo de implementación.
	PE6: R/ Para todas las otras opciones se

	puede y tienen sistemas de asistencia. Sin embargo, en los sistemas que dependen del factor humano en un 100%, se ha observado una alta incidencia a fallas al realizar los pasos o omisión completa del proceso mismo. Lo cual conlleva a inconvenientes con la renovación de los certificados.
¿Cómo resolvió este problema?	PE5: R/ Trabajando junto al equipo encargado del área de Public Key Infrastructure para desarrollar y documentar guías de automatización para diferentes tecnologías comunes y habilitando office hours semanales para proporcionar ayuda y guía técnica para los dueños de las certificados.
	PE6: R/ Gracias a procesos parcialmente automatizados, la incidencia de fallos debido al factor humano decreció enormemente.
¿Cuánto tiempo te llevó resolver el problema?	PE5: R/ Para alcanzar un nivel de automatización de 90% en la empresa, se toma un aproximado de dos años.
	PE6: R/ Aproximadamente 2 años desde el piloto hasta la implementación en producción de sistemas automatizados.
¿Para solucionar este problema necesitas ayuda adicional? En caso afirmativo, especifique	PE5: R/ Si, el reto se abordó de manera integral, trabajando en conjunto los equipos de PKI, de Major Incident Management, los equipos de soporte de cada aplicación especifica, el proveedor externo de certificados.
	PE6: R/ Si se requiere acompañamiento no solo técnico sino también políticas organizaciones que dicten el proceder (gobernanza de TI) y tiempos de implementación para alineación de los grupos organizacionales
¿Cuáles son los pilares de seguridad más afectados al gestionar los certificados manualmente? 1 más - 7 menos	PE5: R/ Disponibilidad. (2) Integridad. (6) Confidencialidad. (5) Autenticidad. (4) No repudio. (7) Seguridad. (1) Privacidad. (3)
	PE6: R/

	Disponibilidad. (X) Integridad. ( ) Confidencialidad. ( ) Autenticidad. ( ) No repudio. ( ) Seguridad. (X) Privacidad. ( )
Describa con amplitud cómo la renovación manual del certificado afecta los pilares de seguridad.	PE5: R/ La renovación manual pone en riesgo la seguridad informática principalmente al reducir la agilidad criptográfica. En caso de una falla de seguridad en la Autoridad Certificador (CA) que provee a la empresa de sus certificados, el departamento de TI se vería obligado a cambiar uno a uno cada uno de los certificados emitidos. En casos de existir muchos certificados, la empresa se vería expuesta a ciber ataques hasta que se complete la revocación de todos. En caso de estar automatizados, este cambio de CA sería tan fácil como cambiar el código de automatización y apuntarlo hacia la nueva autoridad certificadora.
	PE6: R/ La función principal de los certificados digitales es proteger y mitigar los posibles riesgos de seguridad y evitar el acceso no autorizado o la manipulación maliciosa de los datos. Admiten conceptos de seguridad esenciales como autenticación, verificación de identidad y cifrado. Ayudan a establecer confianza, proteger la integridad de los datos y garantizar el cumplimiento de las normas de privacidad de datos. Contar con un proceso manual de renovación de certificados a nivel enterprise representa un alto riesgo. Algunos de los principales riesgos de seguridad de la gestión manual del ciclo de vida de los certificados son: - Mayor vulnerabilidad a violaciones de seguridad. - Costosos tiempos de caídas e interrupciones del servicio causados por certificados caducados u obsoletos. - Retraso en la respuesta ante accesos no autorizados e incidentes de

	seguridad. - Postura de seguridad debilitada debido a una mala configuración del certificado. - Impacto negativo en la reputación de su marca y la experiencia del cliente. - Falta de visibilidad y control centralizados. - Mal uso de los certificados digitales por revocaciones retrasadas o perdidas.

Fuente: Elaboración propia

4.2 Análisis de resultados

4.2.1 Generalidades

Como parte de la investigación y para un mejor entendimiento del contexto se consideró importante obtener información básica técnica de cada organización, debido a esto las primeras cinco preguntas se enfocaron en características de los servidores y aplicaciones que utilizan. Dentro de las características en común que se logran resaltar están:

1- Cada organización administra un total de certificados diferente dependiendo de los servidores que utilizan las aplicaciones.

2- El sistema operativo que predomina y que tienen en común todas las organizaciones es Microsoft Windows Server 2019, sin embargo, hay algunas pocas organizaciones que también utilizan Linux SuSE Enterprise Server.

3- Con respecto a los servidores web utilizados para alojar, implementar y administrar aplicaciones web, al ser la mayoría servidores Windows, tal como se confirma en las respuestas de los expertos se utiliza Microsoft Internet Information Services (IIS), excepto por un par de organizaciones que combinan Microsoft IIS y Apache Tomcat como servidores web.

4- También se logra identificar que únicamente una organización cuenta con aplicación web externa, mientras que todas las demás organizaciones son aplicaciones web internas, las cuales se encuentra localizadas en una red de tipo segura.

5- Se encontró que la renovación manual de cada certificado digital requiere aproximadamente de 30 minutos para una persona con experiencia, sin embargo, una persona que se ha incorporado recientemente a la organización va a requerir una curva de aprendizaje importante hasta llegar a dominar el proceso. Ahora bien, tomando en cuenta que cada organización cuenta con múltiples certificados digitales, este proceso puede ser tedioso y requerir de mucho tiempo, atención al detalle y recursos de parte de la organización. Es importante agregar que este tiempo podría ampliarse debido a potenciales escenarios de fallos o interrupciones en los servicios, por errores en las instalaciones a falta de documentación o vencimientos inesperados de los certificados

4.2.2 Pilares de seguridad y manejo manual de los certificados digitales

Al analizar la información recolectada respecto al control de la fecha de expiración de los certificados digitales emitidos, se logró evidenciar que algunas organizaciones utilizan hojas de cálculo de Excel, otras realizan reuniones mensuales, y en un caso la organización lo maneja semiautomatizado con notificaciones programadas, concluyendo que en todas las organizaciones se administra manualmente. Los riesgos asociados con una gestión inadecuada de los certificados son múltiples y muy altos, por ejemplo, los certificados sin renovar a tiempo resultan en sistemas caídos, causando potenciales daños a la reputación de la organización y pérdida de confianza del cliente.

Una de las principales preocupaciones de las empresas es el crecimiento exponencial del volumen de certificados, combinado con casos de uso cada vez más complejos y una vida útil más corta de los certificados, las empresas continúan luchando por encontrar formas de administrar los certificados digitales de manera eficiente y sin la necesidad de contratar expertos en PKI altamente especializados, eliminando administrar manualmente los certificados usando hojas de cálculo que solo tienen en cuenta los certificados conocidos.

De las personas consultadas, 86% concuerdan que el principal reto asociado al manejo manual de renovación de certificados digitales es que este es sensible a errores humanos, lo cual puede causar sistemas caídos, costos mayores por respuesta a incidentes, dependencia hacia la persona experta en el proceso, dificultades para transferir el conocimiento y documentar adecuadamente. De hecho, las personas entrevistas expusieron los siguientes escenarios ocurridos en sus respectivas organizaciones:

- El certificado fue actualizado a tiempo y de manera correcta, sin embargo, en el repositorio CI/CD estaba referenciando a la versión anterior y esto provocó que el certificado vencido se configurara en producción. Para poder solucionar este incidente fue necesario realizar una instalación nueva no planificada en el servidor afectado y actualizar el repositorio CI/CD, impactando el servicio y consumiendo recursos de la organización por al menos 1 hora.
- Existencia de documentación técnica desactualizada con pasos confusos, lo cual genera inseguridad al realizar la renovación del certificado para un nuevo implementador. Es debido a esto que se requirió de nuevamente documentar, pero más en detalle el proceso de renovación, y así las nuevas personas responsables del proceso se sintieran seguras y cómodas ejecutándolo. Este

esfuerzo les tomo tres días hábiles de horas dedicadas a discusión, documentación y búsqueda de verificación o confirmación con compañeros expertos de otras áreas de negocio.

- En infraestructuras grandes y complicadas, se presenta el reto de renovar muchos certificados que pueden necesitar de equipos de trabajo muy grandes y de mucho tiempo de implementación. En esta ocasión como solución temporal lo que se propuso fue calendarizar reuniones mensuales con el único propósito de realizar revisiones periódicas de las fechas de expiración de todos los certificados digitales conocidos.
- La persona experta de la organización se jubila sin haber realizado una adecuada transferencia de su conocimiento o documentación técnica requerida. Esto significó que se necesitara contactar a esta persona con la cual ya se había finalizado la relación laboral, además se tuvo que solicitar ayuda adicional externa a la organización.

Por otro lado, el 14% restante expresó que el mayor reto del manejo manual de renovación de certificados digitales es poder mantener actualizado el inventario de estos, ya que se encuentran en un constante aumento casi imposible de monitorear. Menciona que en su organización han experimentado sistemas caídos por motivos de certificados no renovados a tiempo y que para poder actualizar o validar manualmente las fechas de expiración de todo el inventario de certificados les toma alrededor de dos meses.

Basado en las respuestas de los expertos se logra observar que las cuatro organizaciones cuentan con un desafío en común, como optimizar las implementaciones de certificados digitales tanto en términos de pilares de seguridad como de rendimiento y rentabilidad. A medida que las organizaciones amplían su

uso de certificados digitales, mantener un rendimiento óptimo sin gastar demasiado en recursos se convierte bastante complejo. La función principal de los certificados digitales es establecer confianza, seguridad, cifrado, integridad de los datos y autenticidad entre dos aplicaciones, un proceso manual de renovación de certificados es poco eficiente y eficaz y representa un alto riesgo de seguridad para las compañías. Dentro de los riesgos que se pueden enfrentar están:

- Mayor vulnerabilidad a violaciones de seguridad.
- Afecta la disponibilidad de los sistemas por posibles interrupciones del servicio.
- Costosos tiempos de caídas e interrupciones del servicio causados por certificados caducados u obsoletos.
- Retraso en la respuesta ante accesos no autorizados e incidentes de seguridad.
- Postura de seguridad debilitada debido a una mala configuración del certificado.
- Impacto negativo en la reputación de su marca y la experiencia del cliente.
- Falta de visibilidad a implementaciones de certificados sin conocimiento y control centralizados.
- Mal uso de los certificados digitales por revocaciones retrasadas o perdidas.

En la actualidad, las empresas modernas están atravesando por una transformación digital, si desean mantenerse exitosas y competitivas deben moverse con rapidez y ser ágiles, es por esta razón que se recomienda una solución innovadora que automatice por completo del ciclo de vida de los certificados digitales, que más allá del ahorro de tiempo, la automatización significa una eliminación de la variable del error humano y una mayor confiabilidad y mejora en el monitoreo. Este software como mínimo debe contar con las siguientes características:

1- Emisión de certificados.
2- Monitoreo y escaneo automático de certificados digitales.
3- Renovación e instalación.
4- Cuente con la capacidad de revertir cualquier implementación fallida automáticamente.
5- Disponibilidad de APIs para poder crear integraciones por ejemplo con active directory.
6- Cuente con capacidades de reporteo.
7- Módulo de notificaciones.

Esta propuesta de plataforma tiene como beneficio reducir todos los riesgos mencionados anteriormente, además ayuda a mejorar la eficiencia y productividad, proporciona ahorros de costos, cumplir con las normas y pueden responder con rapidez y agilidad a medida que el panorama empresarial y de seguridad continúa evolucionando.

Capítulo 5. Propuesta de Solución

Para el Desarrollo de este capítulo se idearon 4 fases, las cuales se presentan a continuación en la figura #7.

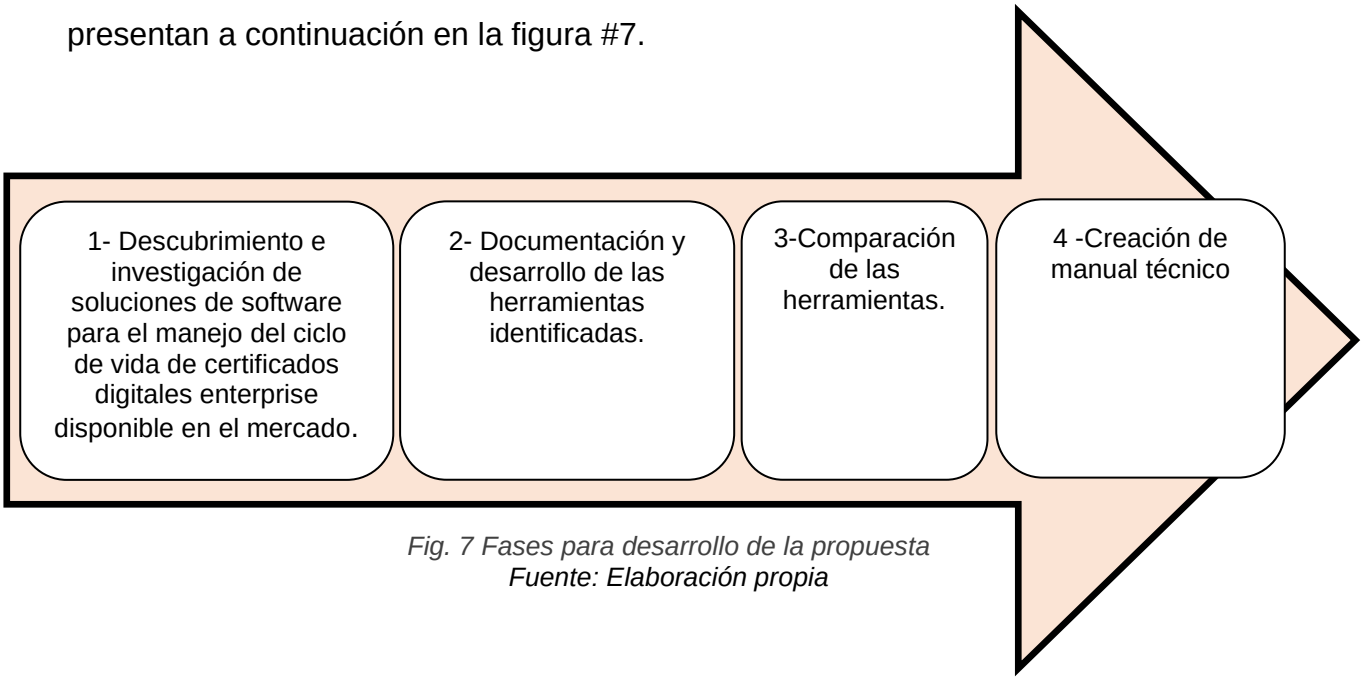


Fig. 7 Fases para desarrollo de la propuesta
Fuente: Elaboración propia

5.1 Descubrimiento e investigación de soluciones de software para el manejo del ciclo de vida de certificados digitales enterprise disponibles en el mercado

Para llevar a cabo esta etapa se acudió a expertos en el área de certificados digitales, profesionales tanto dentro de Intel como profesionales externos, esto con el propósito de obtener criterios diversos y complementarios de profesionales de industrias diferentes. La búsqueda de ayuda de profesionales externos fue con el objetivo de adoptar prácticas basadas en la experiencia y el éxito ya alcanzados por otras organizaciones, organizaciones externas que han enfrentado y solventado algunos de los problemas descritos en la presente investigación.

Al inicio del descubrimiento y la investigación de soluciones empresariales de manejo de certificados digitales se lograron encontrar seis plataformas disponibles en el mercado: GlobalSign, Sectigo, AppViewX, Venafi, KeyFactor y Digicert. Como siguiente paso se realizó un análisis un nivel más profundo de las herramientas, y adicionalmente se tomó la opinión de los profesionales expertos, dando como resultado que las herramientas más competitivas y líderes en el mercado son Venafi y AppViewX, sobre las cuales en las secciones siguientes se desarrollará las características más relevantes de cada una para la aplicación de esta investigación, una comparación entre ellas y finalizar con una evaluación.

5.2 Documentación y desarrollo de las herramientas identificadas

La documentación y desarrollo de las herramientas se basará en los criterios de evaluación del apartado 3.3.3 para la selección final de la solución ideal.

5.2.1 Herramienta Venafi TPP

Venafi es una empresa de ciberseguridad especializada en la gestión de identidades de máquinas. Venafi fue fundada en el año 2004, lo que demuestra su amplia experiencia en el área y una trayectoria de más de 20 años en el mercado de ciberseguridad para las empresas más grandes del mundo. La empresa ofrece una amplia gama de servicios y herramientas destinados a identificar, gestionar y proteger las identidades de las máquinas en redes empresariales e infraestructura de nube. La plataforma de Venafi TPP(Trust Protection Platform) es una solución de gestión de certificados y claves criptográficas empresariales, además automatiza el aprovisionamiento, descubrimiento, monitoreo, validación y administración de certificados digitales y claves de cifrado, desde computadoras de escritorio hasta centros de datos, asegurando las claves criptográficas y los certificados digitales que autorizan y controlan todas las conexiones y comunicaciones de toda la infraestructura empresarial.

La arquitectura de venafi TPP soporta muchas autoridades de certificación (CA), implementaciones de plataformas variadas y varios tipos de cifrado.

5.2.1.1 Escalabilidad

La arquitectura de la plataforma soporta diversas autoridades de certificación, plataformas de implementación y tipos de cifrado. Al tener clientes dentro de los más grandes del mundo, se puede inferir que la herramienta Venafi TPP ayuda a gestionar entornos de infraestructura enormes, diversos y dinámicos gracias a sus características escalables de seguridad y gestión.

Las mejoras de escala y rendimiento introducidas en la versión 18.4 de Venafi Trust Protection Platform demuestran la capacidad de la plataforma para cumplir con los requisitos de las empresas más grandes. Estas mejoras tienen como

objetivo ofrecer escalabilidad y gobernanza eficientes para autenticar identidades de cargas de trabajo en entornos nativos de la nube altamente escalables.

Además, el soporte de la plataforma para una arquitectura de alta disponibilidad en escenarios de desastre y tolerancia a fallas enfatiza su capacidad para manejar operaciones de misión crítica a gran escala, al tiempo que garantiza la continuidad y confiabilidad de las claves criptográficas y los certificados digitales.

Venafi Advanced Key Protect, como complemento de la plataforma Venafi, ofrece una solución escalable para superar los desafíos operativos relacionados con la seguridad de claves y certificados digitales. Esto enfatiza la escalabilidad de las soluciones de Venafi destinadas a administrar claves criptográficas en cargas de trabajo empresariales.

5.2.1.2 APIs/Automatización

Dentro de las funcionalidades de integración por medio de APIs disponibles en la plataforma Venafi TPP se logró encontrar:

- HSM REST: Venafi se ha diseñado para funcionar sin problemas con módulos de seguridad de hardware (HSM) de varios proveedores de renombre como Entrust nShield, Thales SafeNet Luna SA y Securosys Primus HSM. También se integra con Advanced Key Protect, que está diseñado para funcionar con HSM específicos como Entrust nShield Connect HSM y Thales SafeNet Luna SA. Además, los requisitos para poder soportar HSM son constantemente evaluados y documentados.
- API histórico: La plataforma proporciona una API para recuperar información histórica y trazabilidad de certificados.
- Web SDK REST: las API REST brindan acceso a los datos de la solución a través de solicitudes y respuestas con formato JSON. El SDK web de Venafi

TPP es un conjunto de API REST que le permiten automatizar la gestión de certificados. Adicionalmente de los API REST que Venafi proporciona, esta herramienta ofrece integraciones de código abierto. Algunas de las funciones más básicas que se puede desarrollar con Web SDK rest están:

a. Generar un token
b. Importar certificados
c. Puede utilizar un visor Open API.
d. Buscar y generar certificados
e. Registrar un certificado
f. Borrar datos
g. Revocar un certificado
h. Renovar un certificado

- Auth REST SDK: Esta API se utiliza para otorgar acceso y administrar tokens.
- CodeSign Protect: Esta API permite realizar llamadas a la API REST para administrar configuraciones globales, plantillas, proyectos, aplicaciones de firma y permisos.
- Estadísticas de uso: La plataforma cuenta con una API de estadísticas de uso, Venafi TPP recopila información estadística sobre su uso para brindarle funciones que le ayudarán a utilizar el producto. Beneficios incluidos:

a. Nuevas alertas de parches de Venafi para su versión específica de Venafi TPP.
b. Notificaciones de seguridad en tiempo real.
c. Ayuda interactiva y guía de capacitación.
d. Nuevas funciones basadas en datos de comportamiento.

Para brindar estos beneficios, Venafi recopila información sobre el uso de funciones y el comportamiento del usuario en la consola web, así como en los API endpoints que utiliza.

- APIs de código abierto de Venafi en GitHub: Venafi cuenta con más de quince repositorios de GitHub, proyectos de código abierto que puede implementar en su entorno.

5.2.1.3 Integraciones

En la tabla #21 se enumera todos los tipos de integraciones (CA, dispositivos, aplicaciones, servicios, etc.) que son compatibles con Venafi Trust Protection Platform.

Tabla 21 *Venafi TPP Integraciones*

Proveedor	Producto	Tipo de integración
Amazon	Amazon Certificate Manager (ACM)	Autoridad Certificadora
Amazon	Amazon Web Services (AWS)	Servicios en la nube
Apache	HTTP Server	Aplicación
Bouncy Castle	Clients using BC bcpkix library	Certificate Enrollment via EST Protocol
Cisco	IOS	Certificate Enrollment via EST Protocol
Cisco	libest (Client)	Certificate Enrollment via EST Protocol
Citrix	NetScaler VPX	Dispositivo de red
Citrix	NetScaler MPX w/HSM	Dispositivo de red
CyberArk	Enterprise Password Vault	Proveedor de credenciales
Dell	iDRAC 8 (using RACADM 8.3)	IoT
DigiCert	DigiCert CertCentral	Autoridad Certificadora
Entrust	Entrust Certificate Services	Autoridad Certificadora
Entrust nShield	Entrust nShield Connect HSM	HSM
F5	Big-IP Local Traffic Manager (LTM) / Application Delivery Controller (ADC)	Dispositivo de red
GlobalSign	GlobalSign MSSL	Autoridad Certificadora

Hewlet-Packard (HP)	iLO 4 (using HPQLOCFG 1.5)	IoT
HydrantID	HydrantID	Autoridad Certificadora
IBM	Sterling Connect:Direct with Secure+	Application
IBM	WebSphere DataPower IDG	Aplicación servidor web
IBM	Global Security Kit (GSK)	Keystore
Imperva	MX	Appliance
Microsoft	Internet Information Services (IIS)	Application
Microsoft	Active Directory Certificate Services	Autoridad Certificadora
Microsoft	Azure	Servicio en la nube
Microsoft	Windows Certificate Store (CAPI)	Keystore
Mozilla	Network Security Services (NSS)	Keystore
OpenSSL	OpenSSL CA	Autoridad Certificadora
OpenSSL	PEM	Keystore
OpenTrust	Enterprise PKI	Autoridad Certificadora
Oracle	Sun Java System Web Server / Oracle iPlanet Web Server	Aplicación
Oracle	Java Keystore (JKS and JCEKS)	Keystore
Palo Alto Networks	Next Gen Firewall	Appliance
QuoVadis	QuoVadis	Autoridad Certificadora
RedHat	Red Hat Certificate System	Autoridad Certificadora
Riverbed	SteelHead WAN Optimizer	Appliance
RSA Security	RSA Certificate Manager	Autoridad Certificadora
RSA Security	PKCS	Keystore
Sectigo	Sectigo Certificate Manager (CCM)	Autoridad Certificadora
Symantec	Symantec Managed PKI for SSL	Autoridad Certificadora
Symantec	DigiCert PKI Platform	Autoridad Certificadora
Symantec	SSL Visibility Appliance	Network Appliance
Thales	Estclient	Certificate Enrollment via EST Protocol
Thales	SafeNet Luna SA	HSM
VikingCloud	VikingCloud	Autoridad Certificadora
Progress	Chef	Aplicación
Ansible	Red Hat	Aplicación

Puppet	Puppet Inc	Aplicación
Docker	Terraform	Aplicación
HashiCorp Vault	HashiCorp	Aplicación
Github	Microsoft	Aplicación
Kubernetes	OpenSource	Aplicación

Fuente: Elaboración propia

5.2.1.4 Arquitectura

El siguiente diagrama ilustra el proceso de arquitectura, implementación, configuración y uso de Venafi TPP para gestionar certificados y claves en empresas.

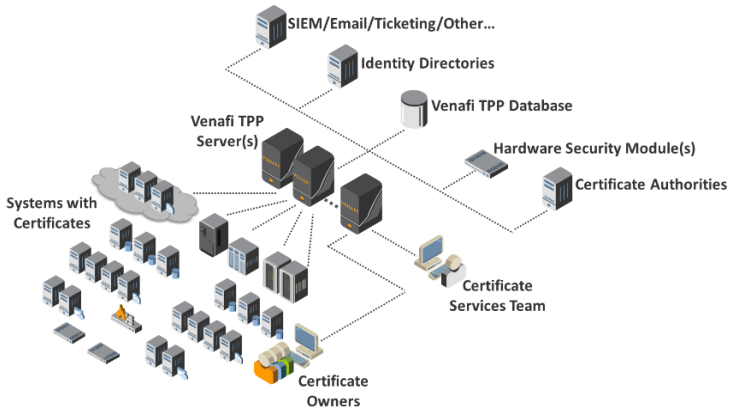


Fig. 8 Venafi TPP Arquitectura.

Fuente: National Cybersecurity Center of Excellence, 2024

5.2.1.5 Facilidad de implementación, administración y mantenimiento

Venafi ofrece ayuda profesional a los clientes con el diseño, desarrollo e implementación de sus productos, incluyendo implementaciones personalizadas.

Los ingenieros de software cuentan con amplia experiencia en la herramienta venafi TPP, lo cual permite una implementación más rápida y ágil. Este servicio profesional de implementación puede realizarse de dos maneras distintas, ya sea que el equipo de venafi realiza la implementación por completo o se puede trabajar en conjunto con los clientes.

5.2.1.6 Compatibilidad

Un aspecto clave y distintivo con que cuenta la herramienta es la compatibilidad con varios sistemas operativos, Venafi ofrece una amplia gama de compatibilidades que ayudan a garantizar operaciones seguras y sin problemas para las organizaciones, ya que soporta desde versiones legacy de Windows hasta distribuciones contemporáneas de Linux como RHEL, CentOS y SUSE Linux. La compatibilidad abarca todo el espectro de versiones de sistemas operativos, desde Windows 7 hasta Windows Server 2022 y actualizaciones de Service Packs y parches. Es importante señalar que la arquitectura de 64 bits es compatible con la mayoría de las plataformas y que IPv6 es compatible con todos los sistemas operativos. El Agente de servidor, que forma parte de la pila tecnológica de Venafi, requiere .NET 4.0 o posterior en todas las versiones de Windows, y existen algunos requisitos adicionales para versiones específicas, como la actualización de Universal C Runtime para Windows 7, 2008 R2, 2012 y 2012 R2.

Venafi TPP admite el uso de Microsoft SQL Server para alojar su base de datos. Con respeto a base de datos y navegadores compatibles están:

- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016 SP2
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012 SP2

- Microsoft Edge (Chromium, última versión)
- Google Chrome (última versión)
- Firefox 78 ESR

5.2.1.7 Innovación

La plataforma de Venafi cuenta con una funcionalidad única de mejora de la experiencia del cliente, cuando se instala Venafi TPP, se recopilan ciertos datos de telemetría. Esta información se utiliza para el cumplimiento de la licencia y permite recopilar información de identificación no personal sobre cómo utiliza el producto.

A cambio, recibirá notificaciones automáticas de eventos importantes (como la disponibilidad de actualizaciones de software), así como ayuda mejorada dentro del producto. Venafi utiliza los datos recopilados a través de esta función para tomar decisiones sobre futuras mejoras del producto. El Informe de uso es una forma que se recopilan los datos, pero también se recopila datos del navegador mientras los usuarios están activos en el producto.

5.2.1.8 Reportes

Venafi TPP cuenta con un módulo específico de reporteo, este proporciona reportes para ayudar a los administradores a gestionar de forma más eficaz su entorno de cifrado, por ejemplo, administradores puedan determinar las asignaciones de permisos actuales, ver listas de certificados que vencen y revisar el estado de las licencias.

Este módulo cuenta con reportes predefinidos, asimismo permite crear reportes personalizados. Los permisos para acceder a estos se deben definir. Algunos de los reportes predefinidos que cuenta la herramienta están:

- Informe de autoridad certificadora, este reporte contiene detalles relacionados con las autoridades certificadoras (CA). Se proporcionan dos vistas:
    A. Certificados únicos asociados a cada CA por número y porcentaje
    B. Instancias de certificados asociados a CA por número y porcentaje
- Informe de inventario de certificados, este reporte proporciona una descripción general de información crítica y estadísticas sobre los certificados, así poder detectar anomalías o problemas proactivamente y poder responder a tiempo.
- El informe Certificados con atributos idénticos, este reporte muestra los certificados de usuario, dispositivo y servidor que comparten un atributo idéntico con al menos otro certificado. Es decir, este reporte se encarga de reportar certificados duplicados.
- El Informe de usuarios, muestra todos los usuarios que tienen acceso a la plataforma.
- El Informe de vencimiento contiene detalles sobre las próximas fechas de vencimiento de certificados. Las fechas de vencimiento se muestran desde la más urgente hasta la menos urgente, según se definió cuando se generó el informe. Este reporte proporciona detalles sobre los certificados que están a punto de caducar para los equipos que administran las aplicaciones o son responsables de los sistemas en los que están instalados los certificados. Esto ayuda a garantizar que los certificados se renueven y actualicen antes de que caduquen.
- El Informe de longitud de clave contiene detalles sobre la longitud de clave del grupo de certificados que especificó. Las longitudes de las claves se clasifican en orden relativo, de cortas (débiles) a largas (fuertes). La longitud de una clave es la longitud en bits de una clave simétrica o de cada clave de un par de claves

asimétricas. La importancia de conocer este dato es que una mayor cantidad de bits hace que sea más difícil realizar un ataque de fuerza bruta.

- El Informe de licencia, este reporte proporciona un recuento de todos los certificados administrados y sus aplicaciones asociadas, así como SSH administrado y claves simétricas para que los administradores puedan determinar si cumplen con el acuerdo de licencia actual.
- Informe de algoritmo de firma contiene detalles relacionados con los algoritmos de firma digital. Los detalles le ayudarán a evaluar el riesgo y el cumplimiento de la política de seguridad de la empresa.
- Informe del período de validez, este reporte muestra los períodos de validez de sus certificados a efectos de cumplimiento.
- Informe wildcard contiene detalles sobre el uso de certificados wildcard. Los certificados wildcard se muestran en la tabla e incluyen el número total de instancias y los detalles asociados con cada instancia.
- Informe de vencimiento, este Informe de caducidad de certificados muestra todos los certificados administrados que han caducado o que caducarán dentro de los plazos designados en la configuración del informe. Puede generar el Informe de Caducidad del Certificado en formato PDF o CSV.
- Informe Histórico de Certificados, este reporte proporciona opciones para informar el historial de certificados.
    A. El informe tiene opciones de filtrado e incluye el DNs de configuración al que pertenece el certificado.
    B. Puede filtrar el informe para incluir o excluir certificados revocados, incluir o excluir certificados caducados, incluir solo certificados de un conjunto de DNs de carpetas y todos los certificados. Siempre excluye los

certificados que pertenecen únicamente a los elementos de la Papelera de reciclaje.

C. Proporciona una API de almacén secreto para recuperar certificados históricos.

D. Permite exportar en formatos CSV y PDF.

- El Informe de uso, este reporte contiene estadísticas de uso para ayudar a Venafi y al cliente a comprender cómo se utiliza el producto y para tomar futuras decisiones de desarrollo del producto. Estos son los tipos de datos generados en el Informe de uso:

  A. Certificados

  B. Llaves SSH

  C. Agentes

  D. Usuarios

  E. Ambientes

  F. Base de datos

- Informe de valor, es utilizado para estimar los ahorros que ha logrado la organización porque sus certificados están protegidos por la plataforma Venafi. El Informe de valor proporciona una forma rápida e intuitiva de estimar los ahorros de costos proporcionados por la plataforma Venafi. Los ahorros de costos estimados se comparan con el costo de administrar manualmente las identidades de sus máquinas. Puede ejecutar este informe manualmente o puede programarlo y enviarlo por correo electrónico a las partes interesadas.

Venafi ofrece una amplia guía de cómo generar y administrar los reportes disponibles por defecto y cómo crear sus propios reportes personalizados.

5.2.1.9 Industria

Venafi tiene una amplia variedad de clientes en diversos sectores industriales, brindando soluciones para la gestión y protección de identidades de máquina, incluyendo: Salud (por ejemplo, Elevance Healt), Energía y servicios públicos (por ejemplo: British Petroleum), gobierno, tecnología, Servicio financieros para los principales bancos y emisores de tarjetas de crédito de EE. UU., África, Emiratos Árabes Unidos y Reino Unido son clientes de Venafi (por ejemplo, Bank of America), farmacéuticos, Aerolíneas (por ejemplo: Aerolínea Southwest) y compañías de manufactura.

5.2.1.10 Venafi TPP: Análisis y conclusiones

De acuerdo con el diagnóstico desarrollado en el capítulo 4, se induce que la solución idónea para los problemas observados es la automatización completa del ciclo de vida de los certificados digitales, esto permite tomar el control de renovaciones y garantiza que los certificados no caduquen sin conocimiento previo.

Según la investigación realizada de la herramienta Venafi TPP, esta ofrece funcionalidades de automatización que puede ayudar a solucionar y simplificar las operaciones para la gestión del ciclo de vida de los certificados TLS/SSL, entre ellas están:

A - En el apartado 5.2.1.4 demuestra que con Venafi TPP se puede implementar la detección continua e inventario. Con esta funcionalidad se puede crear y mantener un inventario completo actualizado de certificados TLS/SSL, incluyendo tres datos críticos como lo son: a quién pertenece cada certificado, dónde está instalado y cuándo caduca. También puede configurar variables, políticas y flujos de trabajo globales, lo cual nos permite evitar que las unidades de negocio utilicen certificados no autorizados.

B - En el apartado 5.2.1.2, explica los diferentes tipos de APIs que cuenta la herramienta y que permite que se automatice los procesos de renovación. Al automatizar las renovaciones, no sólo se ahorra tiempo, sino que se asegura de que los certificados estén actualizados, evitando tiempos de inactividad causados por certificados expirados.

C - La funcionalidad de integración de Venafi con herramientas DevOps (apartado 5.2.1.3) hace que el trabajo de los desarrolladores sea más fácil. Las integraciones basadas en API permiten automatizar implementaciones de certificados, asegurando estricto cumplimiento de los períodos de validez de los certificados.

D - Las múltiples funciones de reporte en tiempo real con que cuenta la herramienta (apartado 5.2.1.8) son clave para asegurarse de que todos los certificados cumplan los periodos de validez y las políticas de la organización. Las auditorías periódicas en tiempo real ayudan a identificar y rectificar alguna inconsistencia, reduciendo cualquier riesgo cibernético o sanciones por incumplimiento.

5.2.2 Herramienta APPVIEWX Platform

AppViewX inició alrededor de 2009 con un equipo de menos de diez personas con múltiples habilidades y destrezas, quienes tenían una visión clara, es así como lograron crear un robusto producto, líder en el segmento de certificados digitales. En la actualidad, la sede está en Nueva York, y cuenta con presencia en India, Norteamérica, Reino Unido y Australia. Suma más de 15 años de experiencia en el mercado, optimizando el producto y formando relaciones estratégicas con empresas de Fortune 500.

AppViewX CERT+, una solución empresarial de gestión del ciclo de vida de claves y certificados que proporciona detección, inscripción, monitoreo, validación, notificación de caducidad, aprovisionamiento, corrección, generación de reportes y revocación automatizados de certificados SSL/TLS a través de la red que incluyen servidores de aplicaciones, servidores web, ADCs, firewalls y dispositivos móviles. CERT+ ayuda a las organizaciones de TI a gestionar y automatizar todo el ciclo de vida tanto de su PKI interna y PKI externa.

5.2.2.1 Escalabilidad

Basado en la actual investigación, se logra observar que la solución AppViewX CERT+ permite adaptarse a organizaciones de cualquier tamaño, y a cualquier necesidad de las organizaciones, por ejemplo, organizaciones con una combinación de una arquitecturas modular, implementaciones en la nube, soporta ambientes heterogéneos multicloud/ load balancers/firewalls/web servers/containers. La integración con múltiples proveedores y ofrecer una solución SaaS, son razones suficientes que hacen que la aplicación AppViewX CERT+ sea altamente escalable y capaz de adaptarse a las cambiantes necesidades de las organizaciones.

5.2.2.2 APIs/Automatización

Una de las mayores ventajas de AppViewX CERT+ es la automatización que proporciona con APIs, fáciles de usar e integraciones predefinidas, por ejemplo, con Microsoft Active Directory.

CERT+ automatiza todo el ciclo de vida de los certificados, desde la emisión hasta el aprovisionamiento, ofrece una variedad de funcionalidades de automatización y APIs, entre ellas:

- Descubrimiento inteligente: Descubrimiento de certificados, así como de aplicaciones y máquinas en cualquier tipo de entornos, a través de escaneos de

dispositivos y de escaneos de direcciones IP en la red. Escaneo autenticado/sin autenticación de dispositivos, autoridades de certificación (CA) y cuentas en la nube.

- Inventario de certificados e información: Un inventario centralizado de certificados descubiertos con una visión holística de la información, Chain of trust, ubicación, fechas de vencimiento de certificados y criptografía. Este módulo centralizado de certificado cuenta con dos opciones de seguimiento del inventario de certificados: Administrar y Monitorear. El modo monitorear únicamente permite visualizar informes y recibir alertas sobre el estado de caducidad y validez de los certificados, mientras que el modo administrar adicionalmente de alertar permite tomar acciones como enviar, revocar, renovar, etc.
- Automatización de extremo a extremo y autoservicio del ciclo de vida del certificado: Automatización del ciclo de vida de los certificados de extremo a extremo desde la inscripción/solicitud, al aprovisionamiento y renovación con flujos de trabajo y tareas de automatización personalizables. Simples métodos de autoservicio para gestionar y solicitar certificados desde un módulo centralizado para mejorar la productividad.
- Amplias integraciones nativas: Integraciones basadas en APIs con múltiples CA (CA públicas y privadas), servicios en la nube, herramientas DevOps, ITSM, SIEM y MDM. Soporte de protocolo de inscripción automática: EST, SCEP, ACME y la inscripción automática de Windows.

Estas funcionalidades reflejan la capacidad de la solución para simplificar y optimizar el proceso de manejo de certificados, brindando a las organizaciones la

posibilidad de ahorrar costos, garantizar una fácil auditoría y cumplimiento, y mejorar la agilidad del equipo mediante el autoservicio.

5.2.2.3 Integraciones

AppViewX ofrece una amplia gama de integraciones nativas con diversos productos y servicios para abarcar las necesidades de automatización, gestión de identidades y seguridad de las organizaciones. AppViewX permite integraciones con soluciones empresariales de terceros a través de API y protocolos de inscripción para automatizar la gestión de certificados en entornos DevOps, multicloud y en contenedores.

Tabla 22 *AppViewX Integraciones*

Proveedor	Producto	Tipo de integración
Google	Google Cloud Platform	Servicios en la nube
Amazon	Amazon Web Services (AWS)	Servicios en la nube
PagerDuty	PagerDuty	Aplicación
Apache	HTTP Server	Aplicación servidor web
Cisco	IOS	Certificate Enrollment via EST Protocol
Cisco	libest (Client)	Certificate Enrollment via EST Protocol
Citrix	NetScaler VPX	Dispositivo de red
Citrix	NetScaler MPX w/HSM	Dispositivo de red
CyberArk	Enterprise Password Vault	Proveedor de credenciales
PrimeKey	EJBCA PKI by PrimeKey	Autoridad Certificatory
Brocade	Brocade	Aplicación
DigiCert	DigiCert CertCentral	Autoridad Certificadora
ENTRUST Solutions Group.	Entrust Certificate Services	Autoridad Certificadora
Let's Encrypt	Let's Encrypt	Autoridad Certificadora
GoDaddy	GoDaddy	Autoridad Certificadora
InCommon	InCommon	Autoridad Certificadora
Entrust nShield	Entrust nShield Connect HSM	HSM
GlobalSign	GlobalSign MSSL	Autoridad Certificadora
IBM	WebSphere DataPower IDG	Aplicación servidor web

Microsoft	Internet Information Services (IIS)	Aplicación servidor web
Squid	Squid	Proxy
VitalQip	VitalQip	DNS/IPAM
Microsoft	Active Directory Certificate Services	Autoridad Certificadora
Microsoft	Azure	Servicio en la nube
Microsoft	Microsoft Active Directory	Aplicación
Oracle	Sun Java System Web Server / Oracle iPlanet Web Server	Aplicación servidor web
Palo Alto Networks	Next Gen Firewall	Firewall
Infoblox	Infoblox	DNS
BlueCat	BlueCat	DNS
Radware	Radware	ADC
BIND	BIND	DNS
AVI Networks	AVI Networks	Aplicación Load Balancers
QuoVadis	QuoVadis	Autoridad Certificadora
Sectigo	Sectigo Certificate Manager (CCM)	Autoridad Certificadora
Trustwave	Trustwave	Autoridad Certificadora
Thawte	Thawte	Autoridad Certificadora
GeoTrust	GeoTrust	Autoridad Certificadora
Thales	Estclient	Certificate Enrollment via EST Protocol
SafeNet AT	SafeNet	HSM
Thales	SafeNet Luna SA	HSMS
Ansible	Red Hat	Aplicación
Puppet	Puppet Inc	Aplicación
Remedy Corporation	BMC Remedy	Aplicación
Servicenow	Servicenow	Aplicación
HashiCorp Vault	HashiCorp	Aplicación
Kubernetes	Kubernetes	Aplicación OpenSource
HAProxy	HAProxy	Aplicación load balancer OpenSource
Fortanix	Fortanix	HSM
NGINX	OpenSource	Aplicación Load Balancer
Fortinet	Fortinet	Aplicación
Check Point Software technologies LTD.	Check Point	Firewall

Juniper Networks	Juniper Networks	Firewall
F5 Networks	F5 Networks	Aplicación
Akamai	Akamai	ADC
A10 Networks	A10 Networks	Aplicación Load Balancer

Fuente: Elaboración propia

5.2.2.4 Arquitectura

La arquitectura de AppViewX se centra en facilitar la administración centralizada de Certificados digitales, dispositivos y la protección efectiva de la infraestructura digital a través de asociaciones y soluciones integrales

Fig. 9: AppViewX CERT+ Arquitectura

Fuente: INFO~TECH research group

5.2.2.5 Facilidad de implementación, administración y mantenimiento

A medida que las empresas aceleran sus esfuerzos de transformación digital, el panorama de TI empresarial está creciendo cada vez más híbrido y distribuido. Los datos y las aplicaciones ya no se limitan a los centros de datos, ahora residen en múltiples plataformas en la nube.

La plataforma de AppViewX cuenta con la flexibilidad de poder realizar

implementaciones de diferente maneras o incluso puede ser consumido como una aplicación Cloud (SaaS/PaaS/IaaS):

A- Implementación local: En los propios servidores o máquinas virtuales y centro de datos de los clientes, lo cual brinda mayor control y personalización sobre la funcionalidad y seguridad de la aplicación, pero requiere mayor inversión inicial, experiencia técnica y costos de mantenimiento continuos.

B- Implementación basada en la nube: La implementación basada en la nube significa que se utiliza un proveedor de servicios externo para alojar el backend de la aplicación en sus servidores o centros de datos, como por ejemplo nubes privadas o nubes públicas utilizando AWS, GCP, Microsoft Azure y otros. Implementaciones en la nube reduce los costos iniciales y operativos, así como la complejidad técnica. También se beneficia de la escalabilidad, confiabilidad y disponibilidad de la infraestructura del proveedor de la nube. Sin embargo, se tiene menos control y personalización sobre la funcionalidad y seguridad de la aplicación.

C- Máquinas Virtuales: AppViewX CERT+ puede instalarse en cualquier instancia de máquina virtual que ejecute el sistema operativo CentOS o RHEL.

D- Kubernetes: Como AppViewX CERT+ es una aplicación basada en Kubernetes, también puede instalarse en un entorno gestionado de entorno Kubernetes como EKS, AKS, GKE, RedHat Openshift, Rancher y otros.

E- Implementación híbrida: La implementación híbrida utiliza una combinación de soluciones locales y basadas en la nube para el backend de la aplicación. Brinda más flexibilidad y optimización para el rendimiento, la seguridad y el costo de la aplicación, pero también aumenta la complejidad y los desafíos de integración de la arquitectura.

F- SaaS - Gestionado por AppViewX: Disponible como servicio, AppViewX CERT+ está totalmente gestionado y actualizado por AppViewX. Los clientes pueden crear directamente una cuenta y empezar a utilizarlo. Para conectarse a los segmentos no públicos de la red corporativa sin tener que abrir ningún puerto en el firewall corporativo, AppViewX proporciona un Cloud Connector que debe instalarse en la red privada.

5.2.2.6 Compatibilidad

- Sistemas operativos: La plataforma AppViewX no está limitada a un solo sistema operativo en particular, es compatible con una amplia gama de sistemas operativos para ejecutar sus aplicaciones como por ejemplo desde Windows Server 2008 R2 hasta Server 2019, Linux, macOS. La plataforma es compatible con sistemas basados en x86 con uno o más CPU para todos los sistemas operativos. Esta importante compatibilidad con diferentes sistemas operativos convierte a AppViewX en una solución flexible y versátil para diversos entornos de infraestructura.
- Bases de datos: AppViewX como todas las soluciones requiere una base de datos para almacenar certificados, claves privadas e información de configuración (todas las claves privadas y credenciales se cifran antes de almacenarse en la base de datos), es por esto que AppViewX interactúa con varias bases de datos, esta ofrece una solución integral que abarca múltiples plataformas de bases de datos, lo que la convierte en una herramienta adaptable a una variedad de entornos de infraestructura empresarial. AppViewX es compatible con, pero no se limitan a las siguientes base de datos: Oracle, IBM DB2, MongoDB, Microsoft SQL Server, PostgreSQL, MySQL, MariaDB, Sybase

ASE, Percona, Amazon, RDS, Google Cloud SQL, Azure SQL Database y HPE NonStop SQL

- Navegadores web: AppViewX es compatible con varios navegadores web, como Google Chrome, Mozilla Firefox, Microsoft Edge y Apple Safari. Esta amplia compatibilidad de navegadores permite a los usuarios acceder de forma segura y sin problemas a AppViewX a través de diferentes sistemas operativos y navegadores web.

5.2.2.7 Innovación

La nueva solución AppViewX SaaS simplifica significativamente la gestión del ciclo de vida de los certificados digitales para acelerar la transformación digital y garantizar la seguridad y el cumplimiento normativo, sin dejar de lado todo el costo y trabajo que significa el mantenimiento de la plataforma en una infraestructura local. Como servicios totalmente administrados por AppViewX, este elimina las cargas operativas, reduce los costos de hardware y software y se escala automáticamente para satisfacer las demandas de certificados de cualquier organización.

Los beneficios de las nuevas soluciones AppViewX SaaS incluyen:

- Rentabilidad instantánea: los servicios totalmente gestionados y fáciles de implementar ofrecen resultados en minutos
- Accesibilidad y visibilidad: el control de acceso basado en roles y la accesibilidad remota permiten a los equipos distribuidos gestionar los requisitos de certificados y claves de cifrado.
- Criptoagilidad: responda rápidamente a los problemas, mitigue el riesgo y mantenga el cumplimiento si es necesario volver a emitir, renovar y/o revocar las CA o los certificados.

- Reducción de recursos y costos: elimina la necesidad de aprovisionar costosos hardware y software criptográfico
- Mantenimiento y seguridad: AppViewX mantiene el servicio y cumple con estrictos estándares y prácticas de seguridad para proteger las claves y evitar el uso indebido de certificados.

5.2.2.8 Reportes

La herramienta AppViewX ofrece una variedad de reportes predefinidos que pueden ser utilizados para monitorear y gestionar eficazmente los certificados digitales; como por ejemplo la caducidad de los certificado, estos pueden enviarse por correo electrónico para acciones manuales o mediante el protocolo de gestión de red (SNMP) para la automatización e integración con soluciones como ITSM y SIEM. El módulo de informes preconfigurados proporciona acceso rápido y específico a los datos que necesita para supervisar los datos que necesita para supervisar la infraestructura.

La herramienta permite crear alertas e informes personalizados según las necesidades de la organización. Los usuarios individuales también pueden personalizar su panel de control según sus necesidades.

Todas las acciones importantes relacionadas con el ciclo de vida de los certificados o los cambios de configuración son registradas. AppViewX permite almacenar estos registros de cambios a largo plazo para propósitos de reportes y auditorias.

Algunos de los reportes predefinidos con que cuenta la herramienta AppViewX CERT+ están:

- Reporte de vencimiento de certificados: Muestra la información de los certificados que están por vencer, incluida la fecha de vencimiento, el propietario y el tipo de certificado.
- Reporte de certificados emitidos: Proporciona detalles sobre todos los certificados emitidos, como la autoridad emisora, el asunto, la fecha de emisión y otros metadatos relevantes.
- Reporte de certificados revocados: Enumera los certificados que han sido revocados, la razón de la revocación y la fecha en que se produjo.
- Reporte de conformidad regulatoria: Ayuda a las organizaciones a demostrar el cumplimiento de los requisitos normativos relacionados con la gestión de certificados, como el Reglamento General de Protección de Datos.
- Reporte de uso de certificados: Muestra información sobre cómo se están utilizando los certificados en la infraestructura de la organización, como los servidores, las aplicaciones y los dispositivos que los utilizan.

Estos reportes predefinidos proporcionan a los administradores una visibilidad integral del estado de los certificados digitales en su entorno, lo que les permite tomar decisiones informadas y mantener la seguridad de sus sistemas.

5.2.2.9 Industria

La solución AppViewX cubre una amplia gama de industrias, sin embargo se enfoca principalmente en industrias que dependen en gran medida de la infraestructura de TI y la seguridad de las aplicaciones, industrias como los servicios financieros, los medios, la atención médica y la computación en la nube.

5.2.2.10 APPVIEWX: Análisis y conclusiones

De acuerdo con la información proporcionada en los resultados de la investigación, la plataforma AppViewX Inc. cuenta con muchas funcionalidades claves, sin embargo, entre ellas se destacan tres mencionadas en el apartado 5.2.2.2 que ayudan a solucionar el problema descrito en el apartado de antecedentes del problema. Estas funcionalidades son:

- Descubrimiento inteligente: Esta funcionalidad se utiliza para el descubrimiento de certificados de servidores, clientes y dispositivos ADC a través de diversos modos, como IP, subredes, URL e inicios de sesión de dispositivos gestionados (ADC). Luego los certificados descubiertos se convierten automáticamente en un inventario con la información necesaria adjunta, proporcionando una amplia visibilidad de la infraestructura de certificados.
- Módulo centralizado de certificados descubiertos: Este módulo ofrece dos modalidades de seguimiento del inventario de certificados: Administrar y Monitorear. El modo monitorear le permite ver informes y recibir alertas sobre el estado de caducidad y validez de los certificados, mientas el modo administrar permite realizar más acciones relacionadas con el ciclo de vida de los certificados, como enviar, revocar, renovar, etc., además de las funciones básicas de alertar y elaboración de informes del modo Monitorear. Esta funcionalidad nos proporciona una gestión eficaz de los certificados digitales, implica una supervisión continua de los ciclos de vida de los certificados, nos establece procesos claros para realizar un seguimiento de la emisión de certificados, las fechas de caducidad y los calendarios de renovación.
- Automatización extremo a extremo: Esta solución automatizada de gestión del ciclo de vida de los certificados ayuda a realizar un seguimiento de los ciclos de

vida de los certificados, garantizando renovaciones puntuales y minimizar las posibilidades de interrupciones del servicio a causa de certificados caducados.

La plataforma AppViewX ayuda a los departamentos de TI de las empresas a gestionar y automatizar todo el ciclo de vida de los certificados de manera centralizada. Los diferentes usuarios de la aplicación cuentan con autoservicio y permite configurar flujos de trabajo de automatización que ofrecen verdadera agilidad empresarial.

5.3 Comparación de las herramientas

Cuando se investiga sobre soluciones de gestión del ciclo de vida de certificados de nivel empresarial, se logra observar que existen una gran cantidad de soluciones de este tipo, sin embargo, se identificó que en el mercado existen dos proveedores líderes: Venafi y AppViewX. A nivel de características y funcionalidades, las dos soluciones son prácticamente iguales entre sí. Todas estas soluciones cuentan con las mismas funcionalidades base: descubrir, inventariar y automatizar la gestión de los ciclos de vida de los certificados para reducir el trabajo manual, eliminar las interrupciones y las debilidades de seguridad y promover la agilidad criptográfica. No obstante, para efectos de este proyecto de investigación solo se tomaron en cuenta dos soluciones Venafi y AppViewX, para finalmente seleccionar solamente una.

La tabla #23 resume cada una de las categorías que fueron estudiadas y analizadas para las dos soluciones previamente seleccionadas, para luego con base a esta evaluación poder identificar la solución más robusta e idónea como la propuesta final. Como se logra observar la gran mayoría de categorías obtienen la misma evaluación, excepto por la categoría de implementación, reportes e industria. Para la categoría de implementación Venafi TPP puede instalarse en numerosos

entornos, tanto en entornos físicos, como virtuales, como en la nube, siempre que cumpla los requisitos mínimos de hardware y software; por ejemplo: totalmente físico en las instalaciones del cliente. VMWare ESXi local, en la nube en AWS, en la nube en Azure y en la nube en GCP, sin embarco AppViewX ofrece el producto/solución como un servicio SaaS siendo más flexible. Para la categoría de reporte la cual es una de las categorías críticas en la selección de la solución según la investigación se observa que aun y cuando ambas proveen módulos para crear reportes personalizados, Venafi ofrece una amplia gama de reportes nativos ya listos a utilizar, facilitando el uso de la herramienta. Con respecto a la categoría de industrias, Venafi presenta mayor ventaja ya que se observa que cuenta con experiencia en la industria de manufactura, todos sus clientes se caracterizan por ser los principales competidores en sus industrias. Estas tres categorías de evaluación se detallan más en profundidad en los respectivos apartados

En resumen, Venafi TPP es una solución de nivel empresarial dirigida a empresas con ingresos anuales de al menos 500 millones de dólares, es bastante completa y robusta, líder en el mercado desde hace muchos años. Gracias a esta evaluación y en concordancia con la comparación realizada por la empresa Gartner Peer Insights se decide proponer la solución Venafi TPP como la solución ideal.

Tabla 23: Evaluación de categorías.

AppViewX CERT+	Categoría	Venafi TLS Protect
10	Escalabilidad	10
5	Compatibilidad	5
15	Integraciones	15
5	Arquitectura	5
10	Facilidad de implementación,	9.5

	administración y mantenimiento.	
10	APIs/Automatización	10
14	Reportes	15
4	Industria	5
3	Innovación	3
20	Análisis y conclusiones	20

Fuente: elaboración propia

5.4 Creación manual técnico

Venafi TPP cuenta con un tipo de instalación llamado Windows CAPI e IIS para automatizar instalación de certificados a sistemas Windows IIS por el método de push. Este apartado proporciona una guía amplia y detallada cómo preparar un sistema para recibir automatización push y como realizar la configuración en Venafi. Algunos de los prerrequisitos básicos para implementar la automatización por el método push son:

- Hay que confirmar que Venafi TPP puede conectarse al sistema en el que se instalará el certificado. Esto implica asegurarse de que los firewalls entre Venafi y el servidor de destino permiten el acceso a WinRM y asegurarse de que WinRM está configurado para aceptar conexiones remotas.
- Venafi TPP requiere WinRM 3.0 o posterior para automatizar la gestión de certificados en Microsoft IIS. WinRM está deshabilitado de forma predeterminada en Windows, Se puede habilitar ejecutando uno de los siguientes comandos en el sistema de destino (se requiere un certificado de computadora para habilitar WinRM a través de HTTPS):

```
# When using port 5985
winrm quickconfig
```

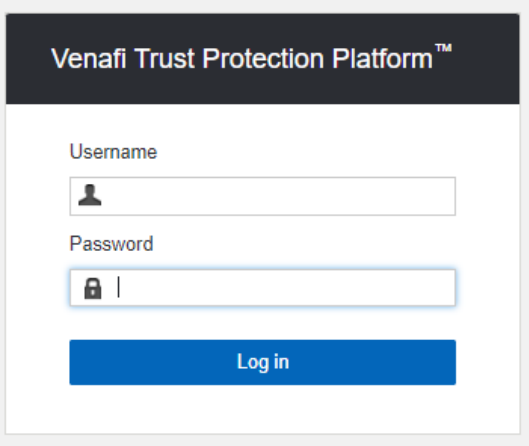
```
# When using port 5986
winrm quickconfig -transport:https

# Run this regardless of port type
Enable-PSRemoting
```

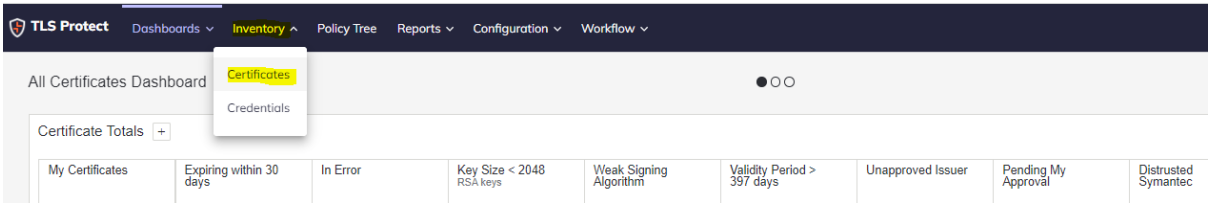
- Cuenta de Venafi, para transportar el certificado entre Venafi y los servidores de destino, será necesaria una cuenta de servicio.

A continuación, se detalla la guía que describe el proceso de configuración del método de instalación push de Windows CAPI & IIS. Aunque esta guía describe cómo configurar también IIS con este método, no requiere configurar IIS en el servidor de destino.

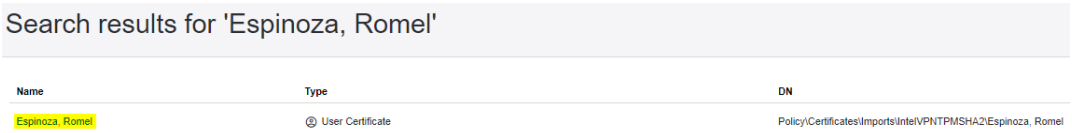
1. Inicio sesión en la plataforma Venafi TPP con las credenciales estándar corporativo para acceder al portal de gestión de certificados.



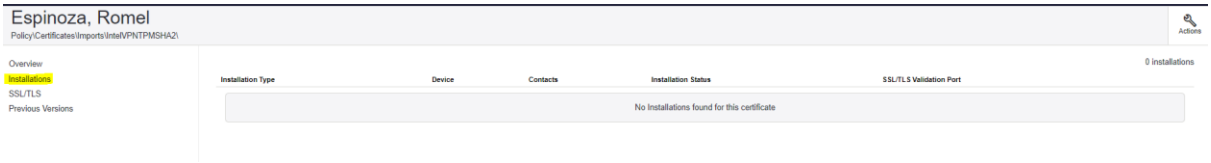
2. Buscar certificado: Busque el certificado existente a automatizar escribiendo el nombre de host en el cuadro Buscar o vaya a la pestaña de inventario, haciendo clic en Inventario>Certificados en la barra de herramientas de Venafi.



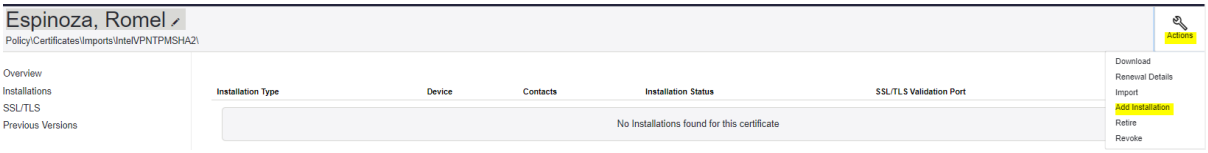
3. Seleccione el certificado a automatizar.



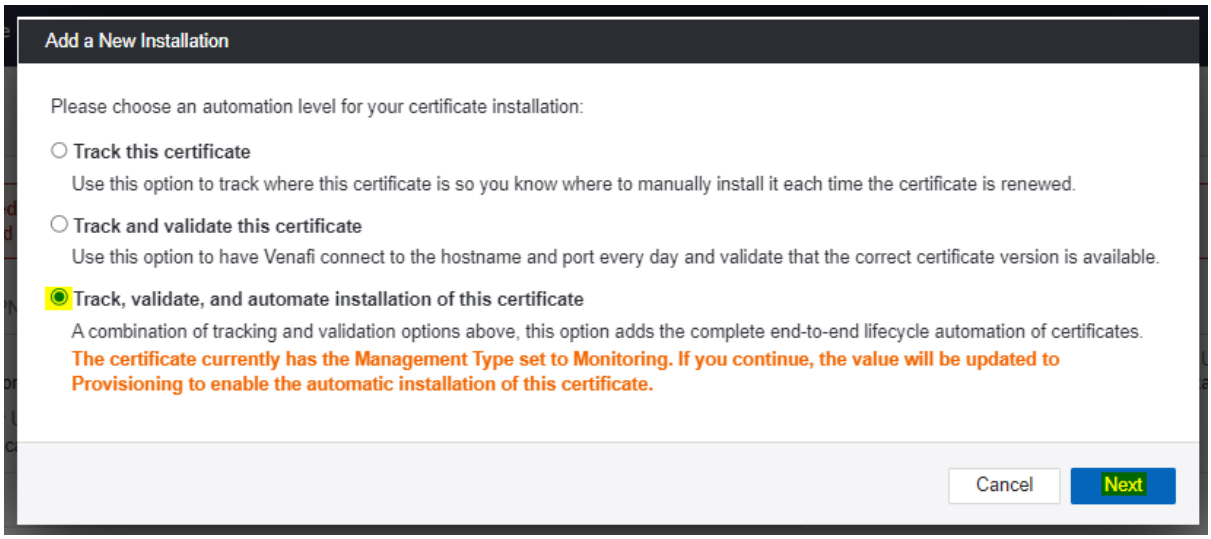
4. Identificar la ubicación de la instalación: Para automatizar la gestión de un certificado, Venafi TPP requiere información sobre la ubicación (instalación) en las que está o estará instalado el certificado. Para ver la información de la instalación configurada para el certificado en Venafi TPP, haga clic en instalaciones en el menú de la izquierda.



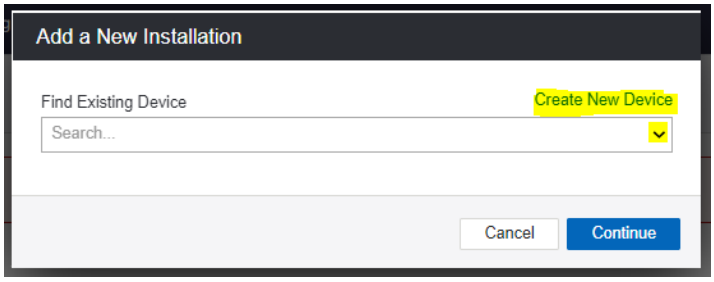
5. Agregar instalación: seleccione añadir instalación en el menú acciones.



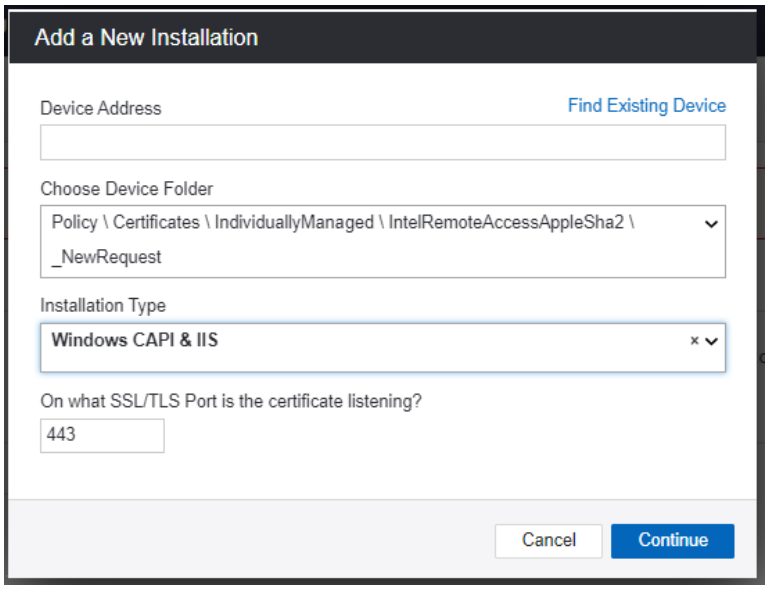
6. Seleccione la opción automatización: En el cuadro de diálogo añadir nueva instalación, seleccione la opción rastrear, validar y automatizar la instalación de este certificado y haga clic en Siguiente.



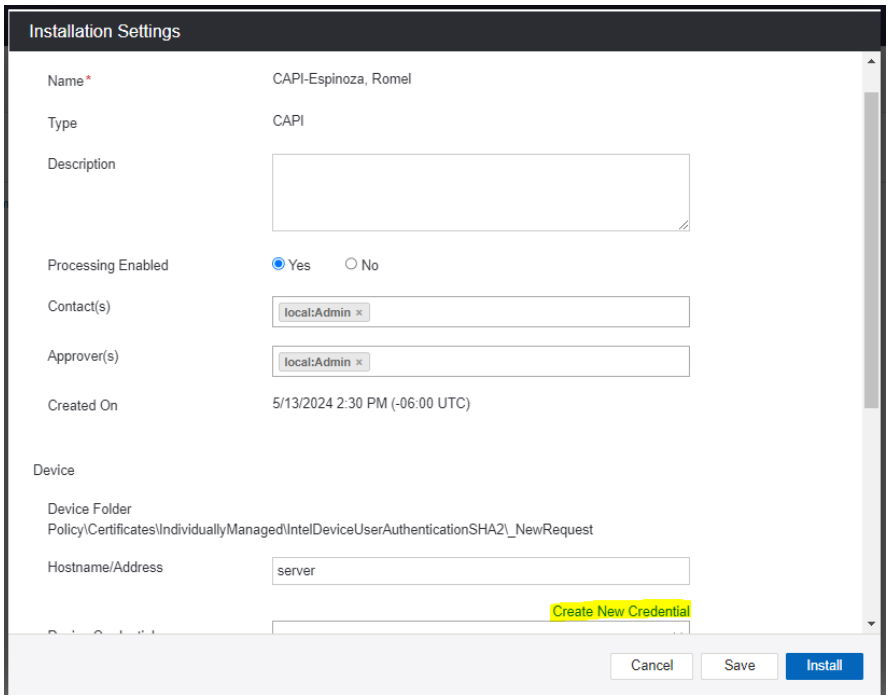
7. Crear un nuevo dispositivo: El primer paso para configurar una nueva ubicación para una certificación es definir la información sobre el dispositivo donde se almacenará. Si ya ha creado una definición de dispositivo, busque el dispositivo en el menú desplegable buscar dispositivo existente. De lo contrario, haga clic en crear nuevo dispositivo.



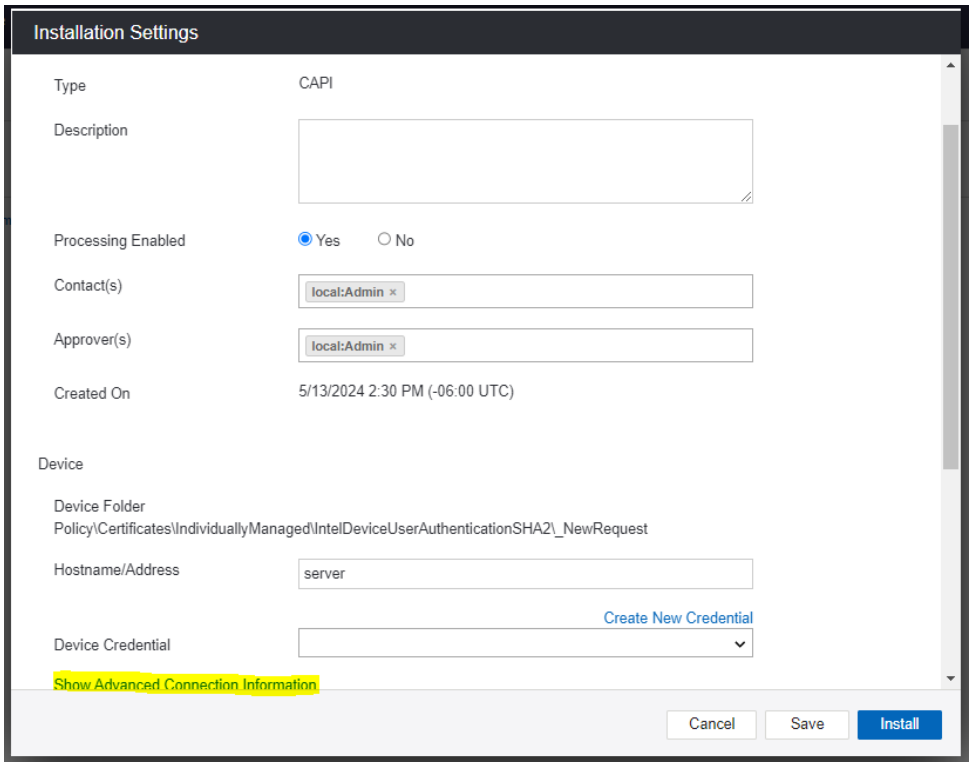
8. Ingresar información del nuevo dispositivo: Al crear una nueva instalación, Venafi necesita crear un dispositivo. El siguiente formulario le pedirá información sobre el dispositivo que recibirá el certificado.



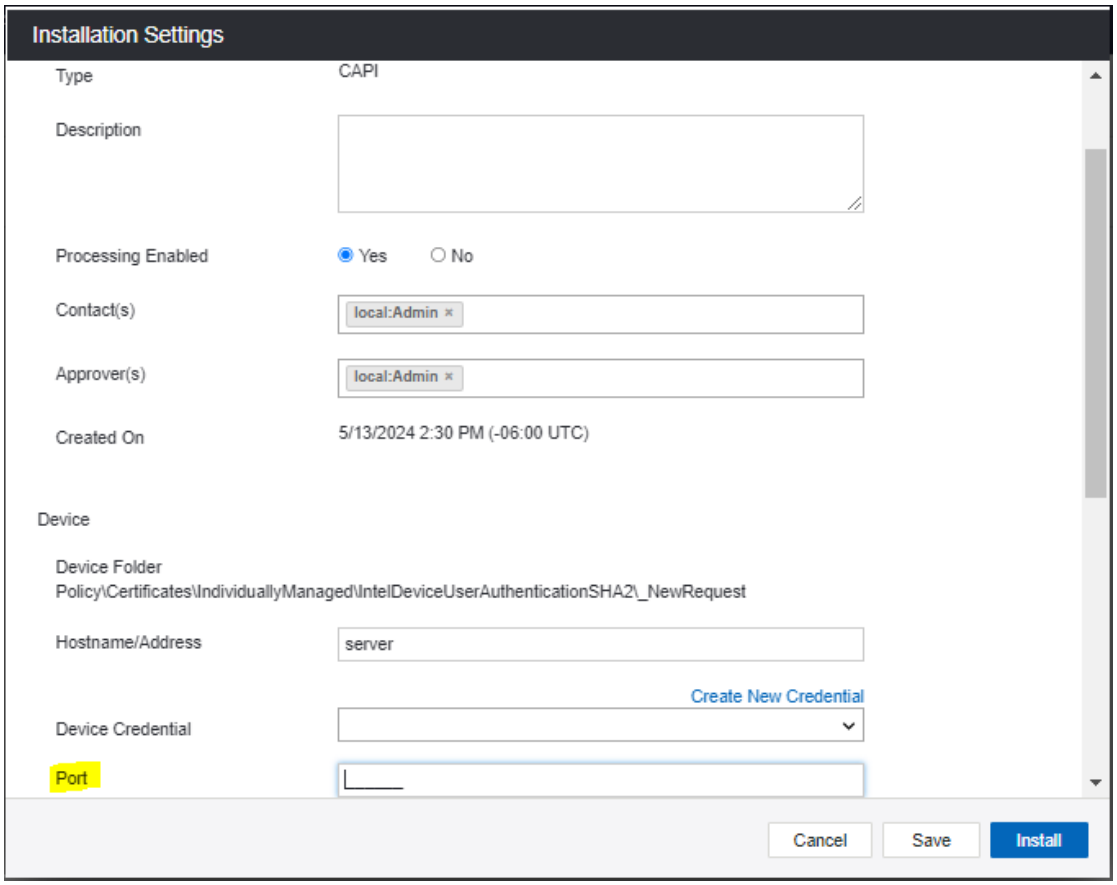
9. Credenciales del dispositivo: A continuación, verá el cuadro de diálogo configuración de la instalación. Busque la credencial.



10. Confirme el puerto: Para automatizar las operaciones de gestión de certificados, Venafi TPP debe iniciar sesión en el dispositivo donde se instalará el certificado. Haga clic en mostrar información de conexión avanzada.

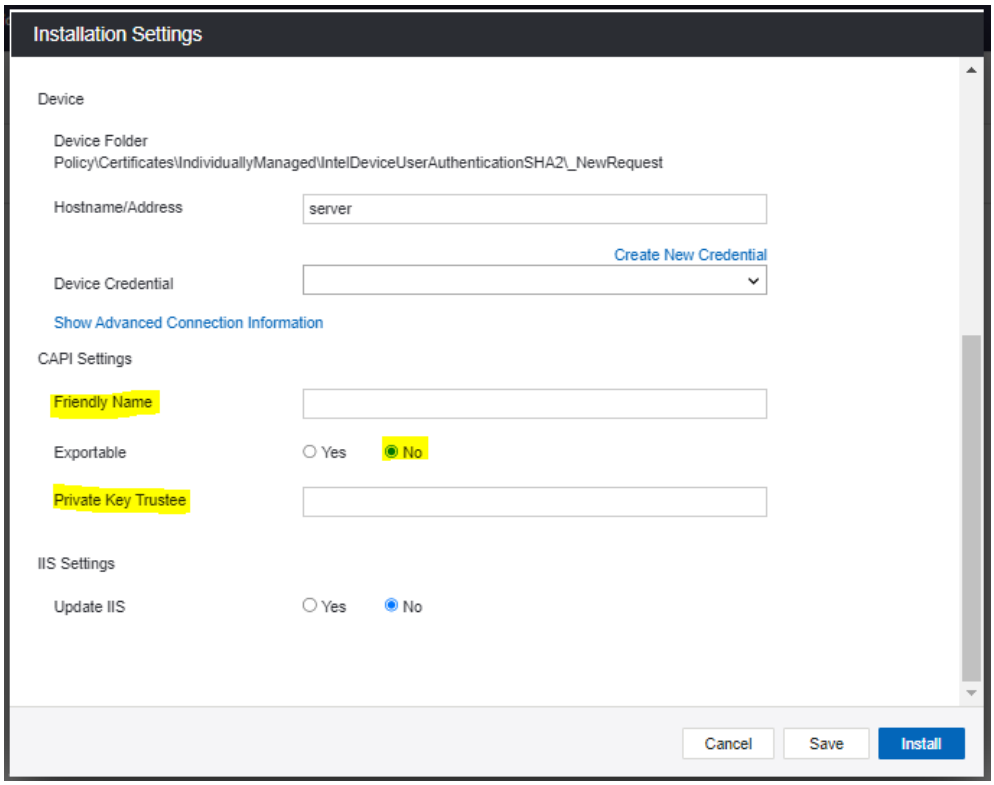


Revise y confirme el puerto configurado en el cuadro de texto puerto.

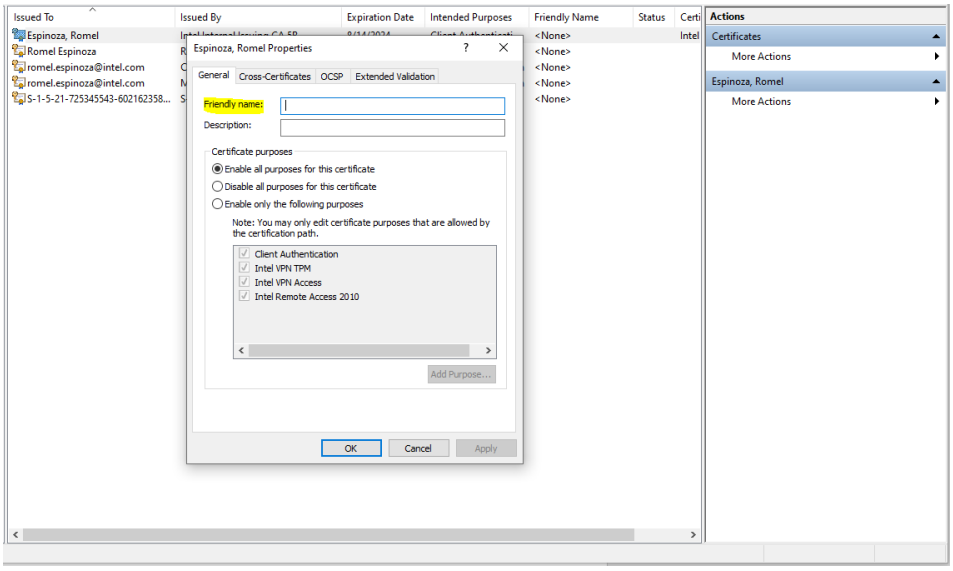


11. Ingresar la configuración CAPI: Vaya a la sección configuración CAPI. En la parte Friendly Name, ingrese nombre DNS primario del sistema donde el certificado va a ser instalados (Es el mismo valor que el nombre común). Si el certificado ya existe, este debe ser exactamente igual, seleccione exportable en No para que la clave privada esté protegida frente a riesgos. Puede dejar el campo Private Key Trustee en blanco a menos que el Grupo de aplicaciones que esté utilizando requiera acceso a la clave privada. Si el grupo de aplicaciones requiere acceso, introduzca el nombre de la cuenta/grupo utilizado por ese grupo de aplicaciones.

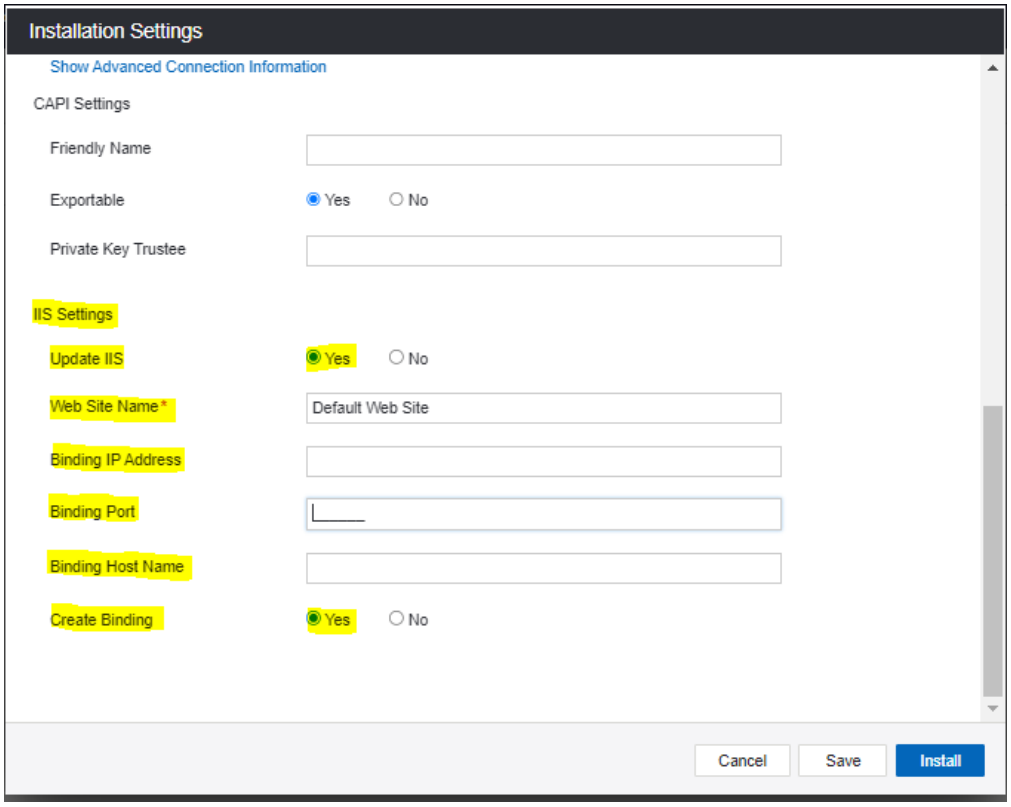
El formato de administrador de clave privada es <Domain>\<Username> or <Domain>\<GroupName> or <LocalGroupName>.



Si no desconoce el Friendly Name o necesita actualizarse, vaya al servidor donde se encuentra el certificado instalado, abra run - mmc, dar clic derecho al certificado y seleccionar propiedades. Asegúrese que tenga el mismo valor que Venafi.

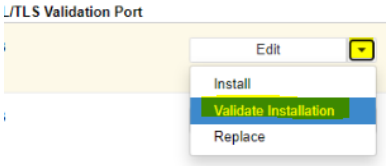


12. Configuración de IIS (opcional): Seleccione la opción Si junto a Actualizar IIS. Si no desea Venafi TPP configure IIS automáticamente, se debe hacer en IIS manager manualmente una vez instalado el certificado.



Puede dejar en blanco Dirección IP de enlace a menos que esté configurando explícitamente la dirección IP del sitio para el enlace al que se asociará el certificado. Para Puerto de enlace, asegúrese de que está configurado el puerto IP correcto. Al igual que con Dirección IP vinculante, puede dejar Nombre de host vinculante en blanco a menos que esté vinculando explícitamente el nombre de host DNS al vínculo que se utilizará con el certificado. Seleccione si en la casilla Crear enlace. Haga clic en Guardar para completar el proceso de configuración de automatización de certificados.

13. Prueba de configuración: En la pestaña de instalaciones busque la instalación recién creada, despliegue el cuadro asociado a su instalación y seleccione validar instalación.



Espere unos minutos y actualice la página. Debería ver validación de instalación exitosa. De lo contrario, haga clic en editar y validar la configuración para la instalación.

Capítulo 6. Conclusiones y recomendaciones

6.1 Conclusiones

A raíz de la realización de este proyecto se logra concluir la existencia de grandes desafíos asociados en la administración de los inventarios de certificados digitales, los altos costos, las capacidades limitadas de administración de certificados, especialmente con dispositivos que no son Windows. Muchas organizaciones no tienen políticas, procesos, roles y responsabilidades claros definidos para garantizar una gestión eficaz de los certificados. Además, no aprovechan la tecnología y la automatización disponibles en el mercado para gestionar de manera eficaz y ágil el creciente número de certificados de servidores TLS. A medida que el número de certificados digitales aumenta, la cantidad de trabajo necesario para gestionarlos se multiplica y cuando los certificados de

servidor TLS no se administran adecuadamente, las organizaciones corren el riesgo de sufrir impactos negativos en sus ingresos, clientes y reputación.

A través de la automatización se puede lograr disminuir el tiempo en instalación por consiguiente menos recursos necesarios para administrar estos certificados y eliminar interrupciones a causa de certificados caducados. Existen cuatro funcionalidades básicas en la automatización de certificados digitales, estos son: el descubrimiento, la implementación, gestión del ciclo de vida y la renovación, sin la gestión automatizada del ciclo de vida de los certificados, es de esperar un fuerte aumento en los riesgos interrupciones relacionadas con certificados TLS/SSL expirados. AppViewX CERT+ y Venafi TPP ofrecen soluciones empresariales competitivas para la automatización del ciclo de vida de los certificados y la gestión de identidades de máquina, ambas compañías cuentan con soluciones robustas integrales para el aprovisionamiento, la gestión y el despliegue de certificados SSL/TLS, la gestión de claves y la gestión de identidades de máquina. AppViewX CERT+ se centra en la automatización de flujos de trabajo visuales y la seguridad de la infraestructura de aplicaciones, mientras que Venafi es conocida por sus extensas integraciones con diversas entidades de certificación, la automatización de la gestión del ciclo de vida de los certificados, sus diversos reportes para auditorías, se puede crear y administrar certificados privados para sus recursos conectados en una ubicación central con un servicio de CA privado, la visibilidad adicional hace que sea más fácil realizar un seguimiento de los certificados emitidos y mantener el cumplimiento. Es por esto y según los requerimientos específicos de la infraestructura de Intel se ha seleccionado como la mejor opción Venafi TPP.

6.2 Recomendaciones

Para abordar eficazmente los riesgos y desafíos organizacionales relacionados con los certificados de servidor TLS y garantizar el buen funcionamiento de estos, se hace necesario hacer un abordaje más integral, no solamente aprovechar las tecnologías actuales de automatización, sino deben definir y establecer un programa formal de gestión de certificados TLS con liderazgo ejecutivo, orientación y soporte. El programa formal de gestión de certificados TLS debe incluir políticas, procesos, roles y responsabilidades claramente definidos para los propietarios de los certificados y el equipo de servicios de certificados, así como un departamento central de certificados. El programa debe ser impulsado por el equipo de certificados, pero debe incluir la participación de los propietarios de los certificados, ya sea que los propietarios de los certificados sean responsables de servidores tradicionales, dispositivos, máquinas virtuales, aplicaciones basadas en la nube, DevOps u otros sistemas que actúan como servidores TLS.

También hay que prestar mayor atención al aumento en el uso de infraestructura en la nube y metodologías/herramientas DevOps, estas crean una dependencia con el protocolo TLS para proteger las comunicaciones, por lo que requiere la implementación de metodologías sólidas de gestión de certificados de servidor TLS. Las versiones futuras se centrarán en estrategias para gestionar eficazmente los certificados de servidor TLS para la nube y DevOps, incluidas estrategias para adaptar las metodologías de gestión a medida que el entorno de nube y las metodologías/herramientas de DevOps sigan evolucionando y cambiando rápidamente.

También es recomendable investigar las mejores prácticas para la gestión de certificados del servidor TLS en el contexto de adquisiciones de empresas, así como

investigar para proporcionar más detalles sobre qué aspectos de la gestión de certificados auditar.

Referencias

ADMWARE. (2018). Gestión centralizada de certificados digitales. https://admware.es/gestor-integral-de-certificados-digitales/

appviewX Inc. (2024). What is Crypto-agility? https://www.appviewx.com/education-center/what-is-crypto-agility/

appviewX Inc. (2024). What is X.509 Standard? https://www.appviewx.com/education-center/encryption-standards-regulations-and-algorithms/what-is-x-509-standard/

Boniface, R., Randall, M., & friendman, J. (2014). US Patent No. 8,719,908 B1. https://patentimages.storage.googleapis.com/18/b9/96/fd86b1133e652d/US8719908.pdf

Chavarría-González, M. C. (2011). La dicotomía cuantitativa/cualitativo: falsos dilemas en la investigación social. *Actualidades en Psicología*, 25, 1-35 https://revistas.ucr.ac.cr/index.php/actualidades/article/view/70/pdf_56

Chokhani, S., Ford, W., Sabett, R., Merrill, C., & Wu, S. (2003). Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. https://doi.org/10.17487/RFC3647

COMODO Inc. (2024). SSL Certificate Security Glossary. https://comodosslstore.com/support/glossary.aspx

Hernández, R., Fernández, C., & Baptista, P. (2010) Metodología de la investigación (5 ed.). McGraw Hill. https://www.icmujeres.gob.mx/wp-content/uploads/2020/05/Sampieri.Met.Inv.pdf

Herrera, J., & Fernández, D. (2006). Certificados digitales. *Acta Nova*, 3 (3), 586-596 http://www.scielo.org.bo/scielo.php?pid=S1683-07892006000200011&script=sci_arttext

Hillier, S., Lee Dilkie, R., & Rosenquist, G. (2000). United States Patent No. 6,055,636. https://www.freepatentsonline.com/6055636.pdf

Hinton, H. M., Falola, D. M., Moran, A. S., & Wardrop, P. R. (2010). United States Patent nº US 7,698,375 B2. https://patentimages.storage.googleapis.com/17/dd/e2/4303bee74744d2/US7698375.pdf

Hudson, J. (2024). Venafi. https://www.venafi.com/solutions/VIA/no-outages

INFO~TECH research group (2024). AppViewX: Beyond PKI Automation – A Comprehensive Machine Identity Management Solution. https://www.softwarereviews.com/research/appviewx-beyond-pki-automation-a-comprehensive-machine-identity-management-solution

Jarvie, J., Vayner, L., & Payne, C. (2013). United States Patent nº US 8473,735 B1. https://patentimages.storage.googleapis.com/pdfs/US8473735.pdf

Muñoz, C. (2015) Metodología de la investigación. Oxford. https://issuu.com/malurojas19/docs/56-metodologia-de-la-investigacion-carlos-i.-munoz#google_vignette

National Cybersecurity Center of excellence (2024). Appendix C Venafi Underlying Concepts. https://www.nccoe.nist.gov/publication/1800-16/VolD/vol-d-appendix.html#appendix-c-venafi-underlying-concepts

Sharif, T., Brace, C., & Garg, N. (2015). United States Patent nº US 9,197,630 B2. https://patentimages.storage.googleapis.com/63/e0/34/1729d61bb81424/US9197630.pdf

Skarda, C. (2013). United States Patent No. 2013/0318353 A1. https://patentimages.storage.googleapis.com/2f/c4/24/17ae805358308e/US20130318353A1.pdf

VERISIGN Inc. (2021). Everything You Need to Know About SSL Certificates https://www.verisign.com/en_US/website-presence/online/ssl-certificates/index.xhtml

Viafirma RA (s.f.). Manual de uso de la RA. https://doc.viafirma.com/ra-register/certificatemanager/index.html