RESULTADOS DE LA EVALUACIÓN DEL NIVEL DE MADUREZ DE LA AUTOMATIZACIÓN DE LOS CERTIFICADOS TLS

Una evaluación de la situación actual de su empresa en términos de madurez de la automatización, nivel de riesgo y oportunidades de mejora.

digicert®

LA FALTA DE AUTOMATIZACIÓN NOS DEJA VULNERABLES

Prácticas modernas recomendadas para la gestión de certificados TLS.

Hoy en día, los responsables de TI dedican más tiempo que nunca a gestionar un número cada vez mayor de certificados TLS y a responder a riesgos, por lo que están buscando formas más eficientes y ágiles de garantizar la seguridad digital de la empresa. Muchos han visto en los productos de automatización de certificados TLS la solución para supervisar mejor sus cargas de trabajo complejas.

La necesidad de automatizar

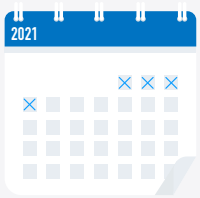
Los expertos en seguridad digital coinciden en que la automatización es la apuesta más segura para las empresas que quieran prepararse de cara a posibles vulnerabilidades. Uno de los principales argumentos a favor es el hecho de que la automatización simplifica las complejas tareas que supone la gestión de certificados. Gracias a herramientas como la función de detección que ofrece CertCentral® de DigiCert, las empresas pueden supervisar e identificar de forma automática cada certificado, esté dentro o fuera de sus redes.

Por otra parte, automatizar el ciclo de vida de los certificados TLS por completo permite a las empresas garantizar la seguridad en todo momento, ya que se evitan las interrupciones ocasionadas por certificados que caducan o quedan obsoletos antes de lo esperado. Además, aquellas empresas que cuenten con una gestión automatizada de todo el ciclo de vida de los certificados estarán preparadas para adaptarse rápidamente a los cambios normativos de gran alcance que se produzcan en el sector —o que introduzca la autoridad de certificación (AC)— y que requieran sustituir o reemitir certificados en poco tiempo, e incluso para un futuro dominado por la criptografía poscuántica. Estas son algunas de las razones por las que las empresas necesitan contar con procesos ágiles y eficientes que les permitan garantizar su seguridad digital.

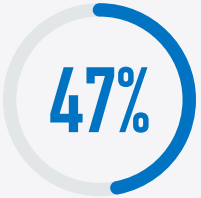
¿Es eficiente su estrategia de seguridad?

DigiCert ha diseñado una evaluación del nivel de madurez de la automatización de los certificados TLS para ayudar a su empresa a evaluar cómo utiliza actualmente las herramientas de detección y automatización, así como a identificar aspectos que podrían mejorarse de cara a reforzar la estrategia de seguridad. Esta evaluación le ayudará a elegir el modelo de implementación más adecuado para su empresa. Ofrecemos soluciones para empresas de cualquier tamaño, sin importar cuántos certificados tengan. Sabemos que cada empresa es única, por lo que creemos que la solución de automatización idónea para la suya será la que mejor se ajuste a sus necesidades y recursos informáticos.

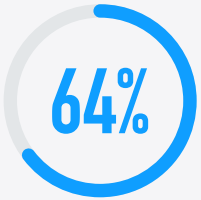
LA SEGURIDAD DIGITAL, EN CIFRAS



Entre 1 y 4 días al mes dedicados a la gestión de certificados.



En promedio, los informáticos dedican el 47 % del tiempo a la gestión de certificados.

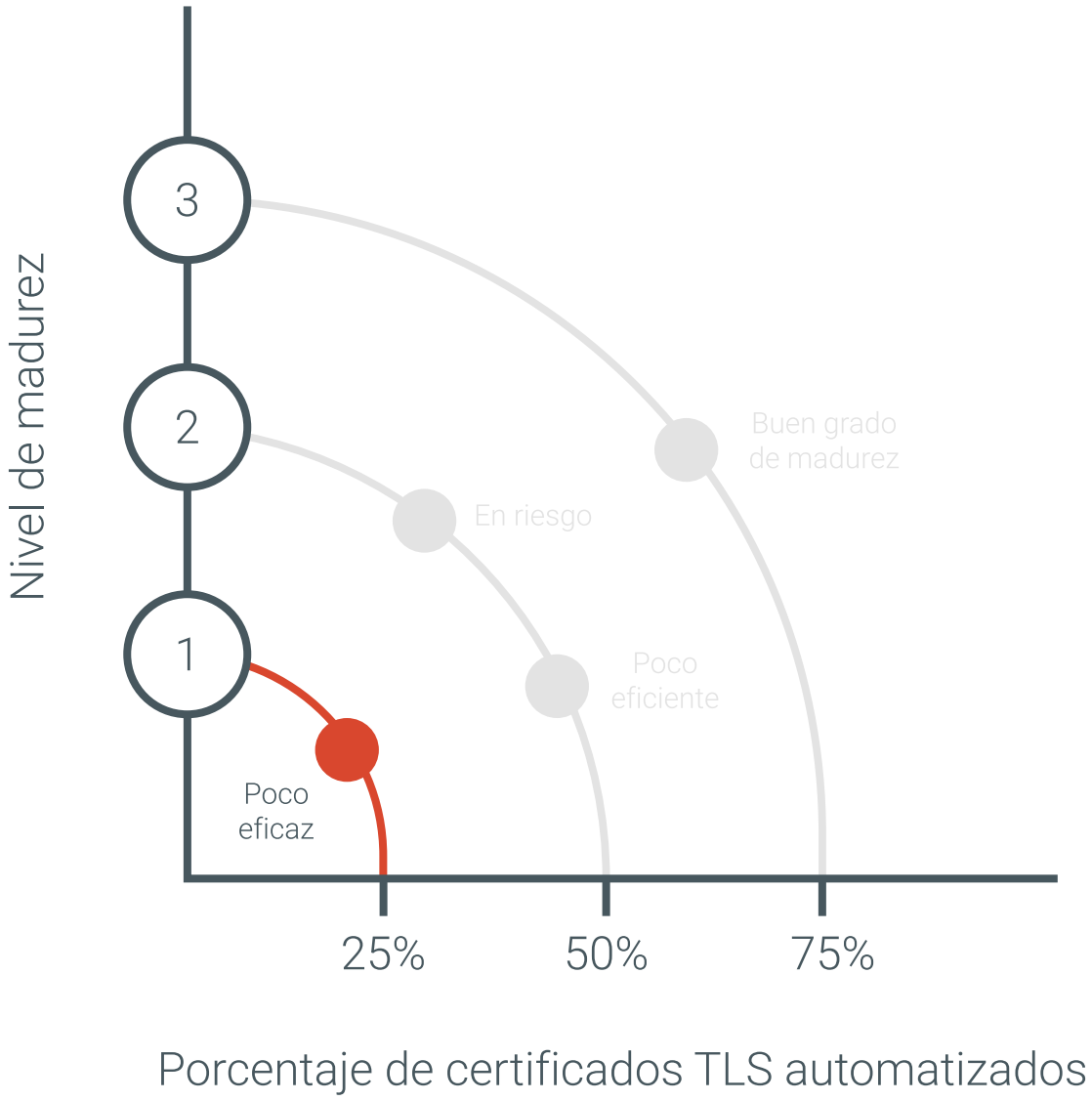


El 64 % encuentra un certificado sin supervisar al mes.

El 38% cree que el tiempo que se necesita para gestionar los certificados es una preocupación importante.

Fuente: Informe de YouGov sobre la automatización de certificados TLS (febrero de 2021)

MODELO DE MADUREZ DE LA AUTOMATIZACIÓN DE LOS CERTIFICADOS TLS



SUS RESULTADOS

Guía para entender su estrategia de seguridad

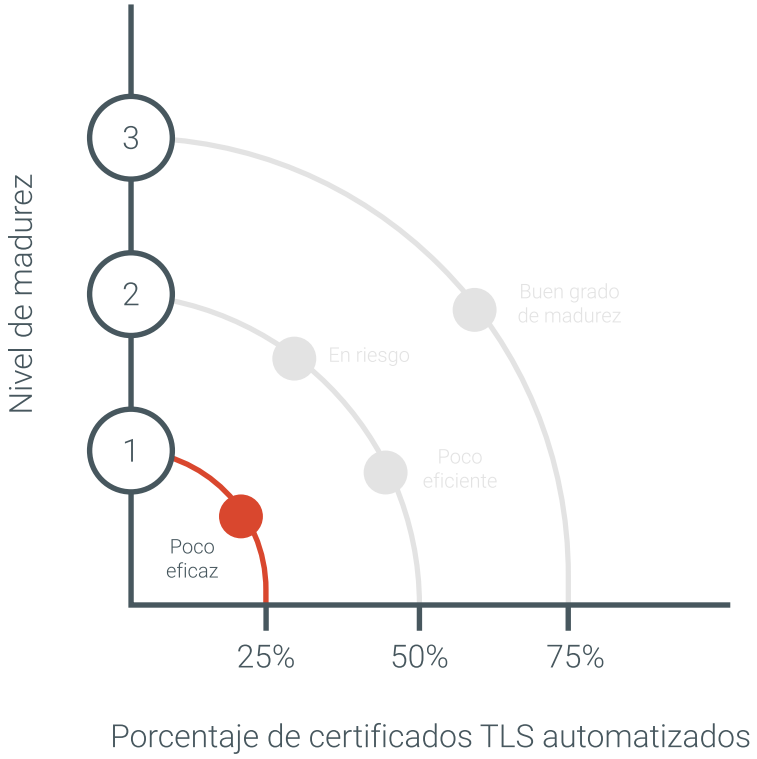
Estrategia de seguridad:

REACTIVA

NIVEL DE RIESGO, EN TÉRMINOS GENERALES: ALTO

Su estrategia actual de gestión de certificados impide a su empresa anticipar posibles vulnerabilidades, cambios introducidos por la AC o interrupciones ocasionadas por incidentes con los certificados. El desconocimiento y la incapacidad de tomar las medidas pertinentes a tiempo constituyen una de las principales amenazas para su sistema de seguridad. Debido al uso de procesos manuales poco eficaces, su empresa se encuentra expuesta a todo tipo de problemas de seguridad.

Si su empresa es una pyme, probablemente lleve un registro de sus certificados, pero podría no estar al tanto de posibles problemas relacionados con ellos (p. ej., certificados mal configurados o claves, conjuntos de cifrado y algoritmos de hash poco seguros). Por el contrario, si es una gran empresa, llevar un seguimiento de todos y cada uno de sus certificados no resulta sencillo, por lo que, cuando se instalan certificados no autorizados en varias áreas de la empresa sin su conocimiento, se generan ángulos muertos y posibles puntos de entrada para los ataques de malware. A este nivel, las empresas se encuentran expuestas a riesgos y tienen altas probabilidades de sufrir interrupciones costosas.



EL CAMINO A SEGUIR

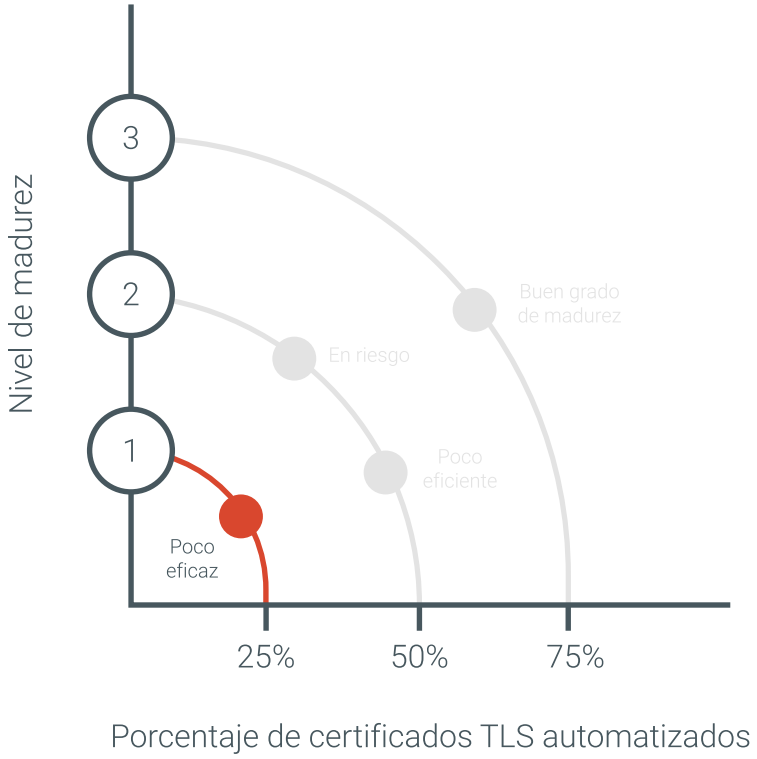
Medidas para mejorar su estrategia de seguridad

Estrategia de seguridad:

REACTIVA

Le recomendamos encarecidamente que tome las siguientes medidas **en los próximos 90 días:**

- Adopte una herramienta de gestión centralizada para sus certificados: CertCentral® de DigiCert le ofrece herramientas para supervisar, emitir, revocar y sustituir todos los certificados desde una única consola.
- Implemente una herramienta de análisis de detección para ver el inventario de sus certificados en su totalidad: realice análisis específicos para estar al día de los cambios que se produzcan en su entorno y obtener valiosa información sobre posibles problemas relacionados con los certificados.
- Céntrese en las prácticas recomendadas para la gestión de certificados TLS: ofrezca información y formación a sus empleados para que sean capaces de llevar un seguimiento de todo el inventario de los certificados de su empresa y de proteger su entorno mediante sistemas de almacenamiento de claves, componentes del ciclo de vida y procesos de desactivación estandarizados, y mediante la supervisión con registros de CT.
- Configure procesos automatizados a gran escala: utilice perfiles, calendarios, alertas e integraciones de terceros.
- Utilice el asistente de automatización de DigiCert, un asistente único en el sector que le ayudará a elegir con facilidad y sin equivocarse el modelo de implementación, la configuración y la instalación que más le convienen.
- Use API: la API REST se puede integrar en cualquier sistema o aplicación que elija. Además, DigiCert cuenta con integraciones de terceros preexistentes.
- En el caso de las pymes, el servicio de ACME gestionado ofrece una herramienta alojada y basada en agente que utiliza el protocolo ACME y facilita la gestión mediante la IU de CertCentral.



EFICACIA DE SU ESTRATEGIA DE SEGURIDAD PARA CERTIFICADOS TLS

Conozca los resultados de su evaluación en comparación con los otros dos resultados posibles

Estrategia de seguridad:
REACTIVA

NIVEL DE RIESGO, EN TÉRMINOS GENERALES: ALTO

Su estrategia actual de gestión de certificados impide a su empresa anticipar posibles vulnerabilidades, cambios introducidos por la AC o interrupciones ocasionadas por incidentes con los certificados. El desconocimiento y la incapacidad de tomar las medidas pertinentes a tiempo constituyen una de las principales amenazas para su sistema de seguridad. Debido al uso de procesos manuales poco eficaces, su empresa se encuentra expuesta a todo tipo de problemas de seguridad.

Si su empresa es una pyme, probablemente lleve un registro de sus certificados, pero podría no estar al tanto de posibles problemas relacionados con ellos (p. ej., certificados mal configurados o claves, conjuntos de cifrado y algoritmos de hash poco seguros). Por el contrario, si es una gran empresa, llevar un seguimiento de todos y cada uno de sus certificados no resulta sencillo, por lo que, cuando se instalan certificados no autorizados en varias áreas de la empresa sin su conocimiento, se generan ángulos muertos y posibles puntos de entrada para los ataques de malware. A este nivel, las empresas se encuentran expuestas a riesgos y tienen altas probabilidades de sufrir interrupciones costosas.

Estrategia de seguridad:
NECESITA MEJORAR

NIVEL DE RIESGO, EN TÉRMINOS GENERALES: MEDIO

El hecho de que su empresa utilice una herramienta centralizada de gestión de certificados TLS/SSL es un buen punto de partida, pero esto no significa que su equipo no pueda seguir mejorando en términos de agilidad para ofrecer soluciones rápidas en caso de interrupción del servicio o incidencias de otro tipo. Si no se utilizan herramientas de automatización, la solución de problemas se complica, se alarga y se vuelve ineficaz, sobre todo en entornos complejos o distribuidos. La red también acusa esa falta de eficacia a la hora de realizar acciones en bloque, como sustituir certificados de proveedores (que suelen estar autofirmados o contener claves poco seguras) o garantizar que se implementen los tipos de certificados adecuados.

En términos de eficacia, no existe una única estrategia de automatización universal, sino que unos modelos de implementación (soluciones locales, en la nube o híbridas) serán más apropiados que otros según el caso.

Estrategia de seguridad:
PROACTIVA Y MADURA

NIVEL DE RIESGO, EN TÉRMINOS GENERALES: BAJO

Cuenta con procesos automatizados eficientes y controlados y con una imagen completa de todos los certificados TLS/SSL de su entorno, lo que permite a su empresa adelantarse a posibles cambios en la industria, interrupciones ocasionadas por los certificados o problemas relacionados con el cumplimiento de la normativa. Las empresas con un buen grado de madurez tienen control sobre todos sus certificados, de los cuales están automatizados hasta el 75 %. Además, han hecho de la automatización una parte integral de sus políticas de seguridad.

Piense cómo podría automatizar hasta el 100 % de sus certificados, de modo que su empresa esté totalmente preparada para las amenazas del futuro (por ejemplo, que sea capaz de sustituir certificados rápidamente en caso de incidente o de adaptarse a un futuro dominado por la criptografía poscuántica).

NUESTRAS RECOMENDACIONES

Conozca mejor las soluciones TLS que debería adoptar

Estrategia de seguridad:

REACTIVA

Le recomendamos encarecidamente que tome las siguientes medidas **en los próximos 90 días:**

- Adopte una herramienta de gestión centralizada para sus certificados: CertCentral de DigiCert® le ofrece herramientas para supervisar, emitir, revocar y sustituir todos los certificados desde una única consola.
- Implemente una herramienta de análisis de detección para ver el inventario de sus certificados en su totalidad: realice análisis específicos para estar al día de los cambios que se produzcan en su entorno y obtener valiosa información sobre posibles problemas relacionados con los certificados.
- Céntrese en las prácticas recomendadas para la gestión de certificados TLS: ofrezca información y formación a sus empleados para que sean capaces de llevar un seguimiento de todo el inventario de los certificados de su empresa y de proteger su entorno mediante sistemas de almacenamiento de claves, componentes del ciclo de vida y procesos de desactivación estandarizados, y mediante la supervisión con registros de CT.
- Configure procesos automatizados a gran escala: utilice perfiles, calendarios, alertas e integraciones de terceros.

Estrategia de seguridad:

NECESITA MEJORAR

Le recomendamos encarecidamente que tome las siguientes medidas **en los próximos 6 meses:**

- Implemente procesos automatizados a la medida de su negocio: DigiCert le ofrece una variedad de soluciones personalizadas que se adaptan a sus necesidades en materia de seguridad: API, URL de ACME, agente de ACME gestionado, automatización con sensores… Y, ahora, también el novedoso Automation Manager.
- Programe análisis mensuales de detección de certificados para los principales dominios web o para los nombres de dominio completos (FQDN).
- Analice sus soluciones TLS para identificar formas de consolidar los sistemas y las partidas presupuestarias: preste especial atención a la innovación, la eficiencia y la optimización de procesos.
- Convierta la automatización en una parte integral de las políticas de gestión de certificados TLS/SSL de su empresa y de los procesos de gestión de su ciclo de vida.
- Utilice el asistente de automatización de DigiCert, un asistente único en el sector que le ayudará a elegir el modelo de implementación adecuado.

Estrategia de seguridad:

PROACTIVA Y MADURA

Le recomendamos encarecidamente que tome las siguientes medidas **en los próximos 12 meses:**

- Siga haciendo de la automatización la política estándar para la gestión de certificados.
- Automatice diversas implementaciones utilizando distintos modelos (p. ej., implementación local o alojada).
- Programe análisis mensuales de detección de certificados para los principales dominios web o para los nombres de dominio completos (FQDN).
- Plantéese utilizar Automation Manager para las implementaciones de certificados de mayor envergadura.
- Garantice la agilidad criptográfica de su empresa mediante el uso continuo de herramientas de automatización que le permitan adaptarse a futuras amenazas, tales como la criptografía poscuántica.

DÉJESE ACONSEJAR POR LOS MEJORES EXPERTOS

Nuestras soluciones de automatización se adaptan a usted. ¿Quiere saber cuál se ajusta mejor a las necesidades de su empresa en materia de seguridad? Póngase en contacto con el gestor de su cuenta o escriba a contactus@digicert.com.

digicert®