digicert®

# LISTA DE PRÁCTICAS RECOMENDADAS PARA LA GESTIÓN DE CERTIFICADOS TLS

En el último año, el 60 % de las empresas ha perdido el acceso a sus aplicaciones críticas debido a un problema relacionado con los certificados.[1] A las grandes empresas, estas interrupciones les cuestan un promedio de 5600 dólares por minuto[2] y, además, dañan tanto su reputación como sus tasas de crecimiento.

Nunca ha sido tan importante adoptar y mantener garantías de protección insuperables que lo ayuden a gestionar los certificados digitales de su empresa.

Por eso hemos reunido esta serie de directrices. Si sigue cada una de estas recomendaciones del sector, su negocio estará a salvo de graves interrupciones consecuencia del desconocimiento o de una cobertura y control insuficientes del ciclo de vida de sus certificados.

# IDENTIFICACIÓN

- [ ] **Haga un inventario de todos sus certificados emitidos**
Sin un inventario estricto de sus certificados, expone a su empresa a distintos riesgos para la seguridad, así que empiece con buen pie y cree una lista de todos los certificados emitidos por su autoridad de certificación (CA). Asegurarse de que todo quede reflejado —desde las CA internas hasta los dispositivos de red— no es tarea fácil y, por eso, la solución más sencilla para detectar sus certificados TLS es utilizar una herramienta de análisis de redes.

- [ ] **Sepa dónde están instalados todos sus certificados**
No basta con tener una lista de certificados emitidos. La instalación de un certificado fraudulento podría causar una filtración de datos cifrados sin que usted se entere. Para evitarlo, es necesario conocer las ubicaciones verificadas de los servidores en los que se alojan sus certificados y agregarlas al inventario.

- [ ] **Identifique a los propietarios de todos los certificados y dominios**
No saber cuándo caducan los certificados es una de las principales causas del aumento de interrupciones relacionadas con estos. Por eso, es importantísimo identificar a los compradores de sus certificados y contar con los procesos necesarios para renovar y transferir la propiedad en caso de que abandonen la empresa.

- [ ] **Compruebe las versiones de las aplicaciones y del sistema operativo del servidor web**
Los hackers pueden explotar ciertos puntos débiles de los sistemas operativos, como por ejemplo Heartbleed: una vulnerabilidad en la biblioteca de criptografía de código abierto OpenSSL que permite a cualquier usuario de Internet acceder a su sistema. Por eso, es fundamental incluir los detalles de sus sistemas operativos y aplicaciones en los inventarios.

- [ ] **Localice los conjuntos de cifrado y las versiones de SSL del servidor web**
Un conjunto de cifrado es una serie de algoritmos que funcionan con el cifrado TLS para proteger las conexiones de red. Los hackers suelen atacar las versiones obsoletas de los certificados TLS o los conjuntos de cifrado sin proteger. De ahí que resulte fundamental que el inventario refleje qué versiones se están utilizando.

[1] https://www.venafi.com/blog/majority-businesses-still-experience-outages-are-you-protecting-your-certificates
[2] https://www.venafi.com/blog/what-if-you-could-guarantee-eliminating-outages-your-organization

# RESOLUCIÓN DE PROBLEMAS

- [ ] **Deshágase de las claves, conjuntos de cifrado y algoritmos de hash que no sean suficientemente seguros**

  Si sus sitios web internos todavía contienen algoritmos hash antiguos, como MD5 o SHA-1, será necesario actualizarlos. En el caso del protocolo TLS, se recomiendan únicamente las versiones 1.2 y 1.3. Asimismo, debe asegurarse de estar utilizando conjuntos de cifrado más modernos, como AES.

- [ ] **Controle la emisión y distribución de los certificados comodín**

  Los subdominios y la facilidad de gestión de los certificados comodín pueden resultar tentadores. Pero es importante tener en cuenta que, si sus claves privadas se ven comprometidas, los hackers pueden manipular cualquier sistema de ese dominio, lo cual dificulta y encarece las revocaciones y las reemisiones de certificados. No obstante, si se cumplen una serie de condiciones estrictas, los certificados comodín pueden ser seguros y flexibles.

- [ ] **Implemente los tipos de certificado adecuados**

  En materia de certificados, es fundamental trabajar con las herramientas adecuadas. No hay ningún problema con utilizar certificados TLS privados para sus sistemas internos. Sin embargo, para los sitios públicos necesitará certificados con validación de empresa (OV) o con validación extendida (EV). Si se está transfiriendo información confidencial, no se recomiendan los certificados básicos con validación de dominio (DV), ya que los niveles de seguridad que ofrecen son insuficientes.

- [ ] **Controle todos los certificados procedentes de un proveedor de forma predeterminada**

  Los navegadores no confían en los certificados de proveedores porque suelen estar autofirmados o caducados, o utilizar claves débiles y, además, no han sido diseñados para utilizarse en una red de producción. Así y todo, las empresas suelen tener miles de ellos. Simplifique la retirada y la sustitución de estos certificados con lo último en herramientas de automatización y una innovadora plataforma de gestión de certificados.

- [ ] **Asegúrese de que todos los servidores web tengan instalados los parches más recientes**

  Proteger sus sistemas operativos y servidores web de los ataques más dañinos según vayan apareciendo pasa por asegurarse de que cuenten con las revisiones más recientes.

# PROTECCIÓN

- [ ] **Estandarice y automatice los procesos de emisión y renovación**
  Evite errores humanos y ahorre tiempo utilizando protocolos automatizados y estandarizados en sus procesos relacionados con los certificados TLS —incluidas la emisión y renovación—. Con una plataforma de gestión de certificados de calidad, resulta sencillo.

- [ ] **Instale y renueve todos los certificados de manera oportuna**
  Es importante que planifique la renovación de sus certificados en función del calendario de su empresa. Le recomendamos que los renueve periódicamente y, como mínimo, 15 días antes de la fecha de caducidad. Para algunas empresas, lo recomendable renovarlos con hasta 90 días de antelación.

- [ ] **Asegúrese de que las claves privadas no se reutilicen cuando los certificados se renuevan**
  Independientemente del tipo de certificado (con DV, OV o EV), reutilizar claves privadas conlleva el riesgo de que estas sean atacadas. Debería crear siempre un par de claves nuevas durante el proceso de renovación.

- [ ] **Instale certificados y claves privadas de forma segura**
  Cree sus claves privadas en una computadora segura y vele por que solo se distribuyan a través de correos electrónicos cifrados en un sistema del que se puedan eliminar automáticamente.

- [ ] **Controle la revocación y eliminación de certificados durante el proceso de desactivación**
  Asegúrese de contar con los procesos adecuados para gestionar la eliminación y revocación de los certificados cuando los sistemas cambian de manos, se retiran o llegan al final de su vida útil.

# SUPERVISIÓN

- [ ] **Escanee las redes para detectar cambios**

  Gestionar los certificados de forma manual es cada vez más complicado: las redes no dejan de cambiar y el volumen de certificados que poseen la mayoría de las empresas está creciendo a pasos agigantados. Utilizar herramientas de análisis de redes le permitirá ahorrar tiempo y mantenerse siempre protegido, ya que podrá detectar cualquier posible problema tan pronto como aparezca.

- [ ] **Compruebe los registros de Transparencia de certificados (CT) para identificar los certificados fraudulentos**

  Si sus certificados públicos no están registrados, sus clientes recibirán un aviso de que pueden ser sospechosos. De modo similar a los informes de crédito, realizar un seguimiento de los registros de CT permite detectar cualquier certificado de origen dudoso y tomar medidas antes de que sus datos o su reputación se vean dañados.

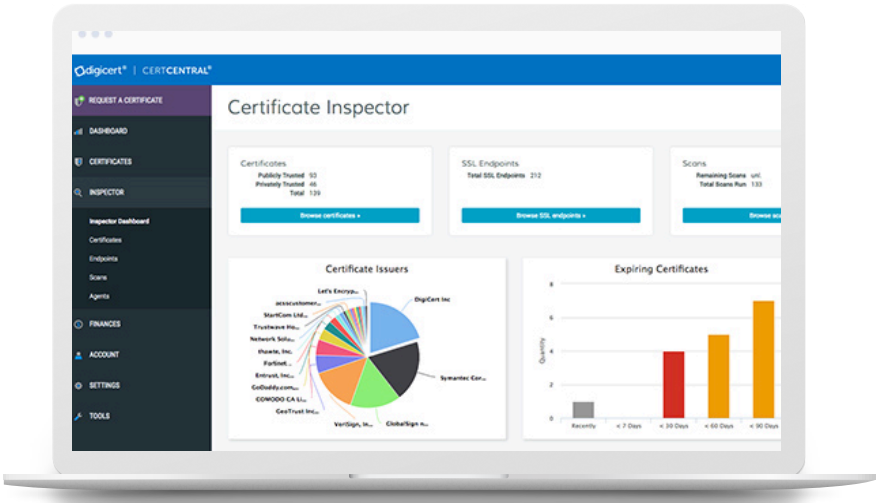
- [ ] **Utilice una autorización de la autoridad de certificación (CAA) para impedir la solicitud de certificados no autorizados**

  Una autorización de la autoridad de certificación es un registro DNS que dicta qué autoridades de certificación pueden emitir certificados para su empresa. Al utilizar una CAA, puede controlar qué CA están autorizadas para emitir certificados para sus dominios, lo que significa que puede evitarse solicitudes de CA no autorizadas o inseguras.

# CONCLUSIÓN

Ahora que tiene claro lo que hace falta para mantener a su empresa a salvo en Internet, es hora de plantearse utilizar la solución más confiable del mercado:

## CertCentral de DigiCert




### Gestione sus certificados fácilmente

CertCentral® de DigiCert le ofrece todas las herramientas y funciones necesarias para identificar, corregir, proteger y supervisar todos sus certificados, además de para personalizar y automatizar todo su ecosistema de certificados. Con ella, podrá:

- Escanear sus redes para saber si se ha producido algún cambio o incorporado algún sistema nuevo.
- Supervisar los registros de CT para detectar certificados no autorizados.
- Utilizar la CAA para detectar solicitudes de certificado no autorizadas y prevenirlas.

Y todo, desde una sola pantalla.

### Para obtener más información, visite digicert.com/certificate-management