GUÍA DE PRÁCTICAS RECOMENDADAS PARA TLS (2022)

Los cinco pilares de la gestión del ciclo de vida de los certificados que ayudan a reducir la carga de trabajo y los riesgos

digicert®

LA IMPORTANCIA DE UNA GESTIÓN DE CERTIFICADOS PROACTIVA

La proliferación y diversificación de los casos de uso de la PKI, motivadas por el crecimiento exponencial del número de páginas web, dispositivos, sistemas, servidores y usuarios que requieren protección y una identidad digital, hacen que sea imprescindible gestionar bien el ciclo de vida de los certificados. Por eso, existen prácticas recomendadas destinadas a mejorar la eficiencia y eficacia de los programas de gestión de certificados para ofrecer la seguridad y la agilidad criptográfica que necesitan las empresas. En este libro electrónico, encontrará un marco detallado y sencillo que le ayudará a mantenerse a la vanguardia en materia de seguridad digital y a cumplir la normativa en todo momento, tanto ahora como en el futuro.

ÍNDICE

DETECCIÓN

Obtenga un inventario completo de todos sus activos criptográficos

Detecte cualquier exposición a exploits conocidos

Analice los conjuntos de cifrado y las versiones de TLS en busca de vulnerabilidades

GESTIÓN Y ELABORACIÓN DE INFORMES

Proteja sus claves privadas

Priorice la corrección

Supervise los certificados comodín emitidos y distribuidos

Implemente los tipos de certificado TLS adecuados

Tenga controlados todos los certificados de proveedor

Asegúrese de que los sistemas estén siempre actualizados

Proteja el acceso a los sistemas de gestión de certificados

Benefíciese de las integraciones con sistemas ITSM

Revise las alertas por si fuera necesario tomar alguna medida

NOTIFICACIÓN

Establezca jerarquías de notificación y derivación

Determine umbrales de notificación

Supervise los registros de Certificate Transparency

Configure alertas de CAA y evite solicitudes de certificado no autorizadas

AUTOMATIZACIÓN

Automatice la gestión del ciclo de vida de los certificados

Logre la agilidad criptográfica automatizando la gestión de certificados

Automatice los procesos empresariales

Personalice las integraciones gracias a las API

UNIFICACIÓN

Disfrute de compatibilidad entre certificados y navegadores en toda la red

Utilice unos servicios de detección e importación que funcionan con cualquier CA

OBTENGA UN INVENTARIO COMPLETO DE SUS ACTIVOS CRIPTOGRÁFICOS

La detección es la base de las prácticas recomendadas para la PKI.

Sin un inventario exhaustivo de todos sus certificados, su empresa podría quedar expuesta a unos riesgos de seguridad que ni se imagina. Utilizar un servicio de detección para encontrar y corregir vulnerabilidades (p. ej., certificados en los que no se puede confiar o certificados que estén a punto de caducar, hashes y claves poco seguras o software de servidor obsoleto) es una de las maneras más eficaces de prevenir posibles interrupciones.

Un buen punto de partida sería elaborar una lista de todos los certificados emitidos por sus autoridades de certificación. Pero ¿cómo saber si lo ha incluido todo en esa lista? ¿Qué hay de sus autoridades de certificación internas y de los dispositivos de red con certificados? Lo primero que convendría hacer es analizar la red en busca de certificados. Otras opciones que tienen las empresas para alimentar su inventario son: inspeccionar sus servidores para detectar cualquier certificado, clave, certificado de usuario y algoritmo; importar raíces privadas e identificar los certificados emitidos a partir de dichas raíces; e importar datos procedentes de otras herramientas de detección.

Conclusión:

Los servicios de detección constituyen el primer pilar de las prácticas recomendadas para la gestión de la PKI, ya que ofrecen una panorámica completa y detallada de los activos criptográficos de la empresa. Se pueden utilizar análisis, inspecciones y otros métodos de detección con la frecuencia que marque la estrategia de mitigación de riesgos establecida, de modo que la detección y corrección de vulnerabilidades no se detengan nunca.

CONFORME UNA VISIÓN UNIFICADA DE SU INVENTARIO:

- Análisis de la red
- Inspección de servidores y archivos
- Detección de raíces privadas
- Importación a partir de herramientas de terceros

DETECTE CUALQUIER EXPOSICIÓN A EXPLOITS CONOCIDOS

Protéjase de los ataques dirigidos a los sistemas.

La información reflejada en el inventario debería incluir, además, los detalles del sistema operativo (como si es Windows o Linux) y de las aplicaciones (p. ej., Apache). Hay que comprobar que todos los sistemas estén actualizados con la versión más reciente para asegurarse de que no sean vulnerables a los exploits.

Es importante hacerlo, porque su empresa podría estar expuesta a exploits graves como Heartbleed, POODLE (SSLv3), FREAK, LogJam o DROWN. También es conveniente evaluar otros aspectos de la seguridad de los sistemas operativos y los certificados de su servidor web.

Conclusión:

Conocer las versiones de los servidores, los equilibradores de carga, los marcos de aplicación, la infraestructura en la nube, las bases de datos y las demás infraestructuras informáticas nos permite tomar las medidas oportunas para prevenir exploits y vulnerabilidades.

ANALICE LOS CONJUNTOS DE CIFRADO Y LAS VERSIONES DE TLS EN BUSCA DE VULNERABILIDADES

Revise los conjuntos de cifrado y las versiones de TLS/SSL.

Normalmente, estos elementos están configurados en los servidores web. Muchos ataques dirigidos a los certificados TLS/SSL ponen el punto de mira en las versiones antiguas de SSL (p. ej., el ataque POODLE dirigido a SSL 3.0) o en conjuntos de cifrado poco seguros (p. ej., el ataque ROBOT contra el cifrado RSA). Nuestra recomendación es utilizar las versiones de TLS más recientes, como las TLS 1.2 y 1.3.

¿Qué es un conjunto de cifrado?

Una serie de algoritmos configurados en un servidor web que ayuda a proteger las conexiones de red TLS/SSL.

PROTEJA SUS CLAVES PRIVADAS

Reutilizar claves es como reutilizar contraseñas, y el ahorro de tiempo no compensa el aumento del riesgo.

Una clave privada es un archivo independiente que se utiliza en el cifrado y descifrado de los datos transmitidos entre el servidor y los clientes conectados. La crea el propietario del certificado durante la solicitud de firma de certificado (CSR). La autoridad de certificación (CA) emisora de su certificado ni crea ni tiene su clave privada; es más, sus administradores son los únicos que deben tener acceso a ella. Como norma general, se recomienda crear un par de claves nuevas para cada certificado. De igual manera, las CSR tampoco deben reutilizarse nunca, ya que al hacerlo se utiliza la misma clave privada automáticamente.

No se olvide de:

- Comprobar si existen claves poco seguras.
- Comprobar si hay alguna clave expuesta.
- Utilizar una caja de seguridad, un token o un módulo de seguridad de hardware para almacenar las claves con un mayor nivel de protección.

Conclusión:

Aunque resulte tentador reutilizar las CSR para ahorrar tiempo, hacerlo duplica las claves y multiplica los riesgos. Automatizar las solicitudes y renovaciones de certificados reduce considerablemente el trabajo manual necesario para generar CSR y aprovisionar certificados.

PRIORICE LA CORRECCIÓN

Corrija cualquier clave, algoritmo de cifrado o hash poco seguro que encuentre en su inventario, así como cualquier activo obsoleto.

Los certificados contienen claves públicas y firmas susceptibles de ser atacadas. Aquellos con longitudes de clave inferiores a 2048 bits o los que utilizan algoritmos de hash antiguos —como MD5 o SHA-1— ya no están permitidos en los servidores web públicos, pero aún podría encontrarlos en sus sitios web internos. De ser así, deberá actualizarlos inmediatamente.

Aún más importante que identificar los certificados con claves o algoritmos de hash poco seguros es revisar las versiones de TLS/SSL y los conjuntos de cifrado que hay en sus servidores web. Deberá contar siempre con las versiones de TLS más recientes, como las TLS 1.2 y 1.3. En el caso de los conjuntos de cifrado, utilice los algoritmos criptográficos más modernos (como el AES). También es recomendable echar un vistazo a esta lista para saber qué conjuntos de cifrado se han quedado obsoletos o ya han sido retirados.

Versiones de TLS/SSL obsoletas y vulnerables:

- SSL v2
- TLS 1.0
- SSL v3
- TLS 1.1

SUPERVISE LOS CERTIFICADOS COMODÍN EMITIDOS Y DISTRIBUIDOS

Los certificados comodín simplifican la emisión de certificados, pero representan un riesgo para la seguridad.

Aunque es innegable que este tipo de certificados suponen una ventaja para los administradores, proteger distintos dominios con la misma clave privada es arriesgado por varios motivos: si, por ejemplo, perdemos o nos roban la clave privada, esta se convierte en la llave maestra para acceder a todos los servidores para los que se emite el certificado. O, si usamos la misma clave privada en toda la red o la compartimos con distintos departamentos, podría acabar perdida o sustraída, con lo que habría que sustituir todos los certificados asociados a ella. Otro ejemplo: si, por cualquier motivo, se revoca el certificado comodín, habrá que actualizar la clave privada en todos los servidores que lo utilizaban, y habrá que hacerlo de una sola vez para no interrumpir la transmisión de datos a través de la red.

Para renovar los certificados comodín hay que seguir el mismo proceso, con lo que, aunque su uso ahorre a las empresas tiempo y dinero en un primer momento, gestionar su renovación o tener que sustituir alguno de repente puede resultar muy trabajoso.

Conclusión:

Si utiliza un certificado comodín, es importante que proteja su clave privada. Para minimizar el riesgo que supone compartir una única clave privada para distintos usos del certificado comodín, debería utilizar una clave privada diferente para cada una de las copias de dicho certificado, además de establecer un sistema seguro para proteger estas claves. También recomendamos aplicar la automatización en cada uno de los servidores en los que esté instalado el certificado comodín. Esto le permitirá ahorrar tiempo, reducir los errores humanos y reducir las probabilidades de que las claves se pierdan.

IMPLEMENTE LOS TIPOS DE CERTIFICADO TLS ADECUADOS

Elija el nivel de seguridad adecuado para su negocio.

Si tiene que proteger un sitio web público que contenga formularios en los que se recoge información sobre los usuarios, o que recopile credenciales y contraseñas, le recomendamos utilizar un certificado de alta seguridad que garantice la integridad de su marca evitando que ni esta ni el sitio web de su empresa puedan falsificarse.

Los certificados TLS con validación extendida (EV) son los que ofrecen las mayores garantías con respecto a la marca y la identidad. Son los que suelen utilizar las administraciones públicas, las multinacionales, los bancos y las organizaciones de servicios financieros. Los certificados con EV están sujetos al proceso de validación más riguroso que existe, que verifica en 16 pasos información como los datos de contacto, el cargo y la función del solicitante del certificado. Además, se realizan diversas comprobaciones: de las listas de contactos bloqueados, de dominio fraudulento y del número de registro, la jurisdicción y el agente registrado de la empresa.

Los siguientes por nivel de seguridad son los certificados TLS con validación de empresa (OV), que validan el propietario del dominio y toda la información de contacto de la empresa. El proceso incluye la verificación de la dirección física de la entidad, una llamada telefónica para comprobar la autenticidad de la solicitud del certificado y comprobaciones de fraude, de malware y de la lista de bloqueados.

Los últimos de la lista son los certificados TLS con validación de dominio (DV), que ofrecen el nivel más bajo de garantías en torno a la identidad y son muy fáciles de falsificar, por lo que no se recomienda utilizarlos en sitios web que manejen información confidencial. En lo que respecta a los certificados TLS privados, suelen utilizarse en sistemas internos; pero, para garantizar la protección, la raíz privada debe extenderse a los usuarios.

CASOS DE USO DE LOS CERTIFICADOS:

VALIDACIÓN EXTENDIDA (EV)

- Bancos y servicios financieros
- Empresas de la lista Fortune 500
- Empresas de la lista Global 2000
- Comercio electrónico
- Cumplimiento normativo (p. ej., HIPAA, PCI)

VALIDACIÓN DE EMPRESA (OV)

- Pantalla de inicio de sesión
- Sitios web comerciales
- Cumplimiento normativo (p. ej., HIPAA, PCI)

VALIDACIÓN DE DOMINIO (DV)

- Blogs
- Sitios web personales
- Cualquier sitio web que no realice transacciones ni recopile información

TENGA CONTROLADOS TODOS LOS CERTIFICADOS DE PROVEEDOR

Los certificados de proveedor atienden más a la facilidad de uso que a la seguridad.

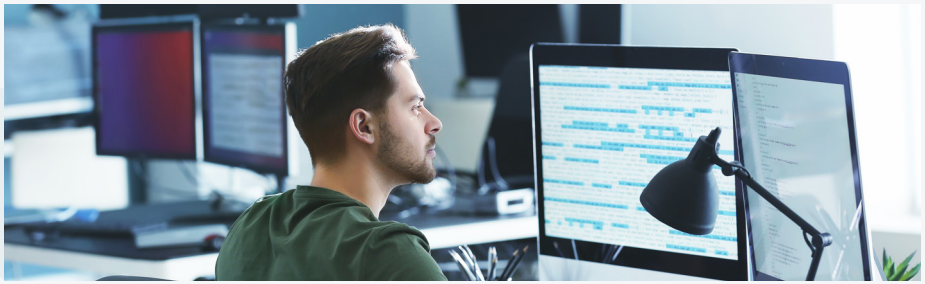
Los emiten proveedores de hardware externos y vienen preinstalados en sus dispositivos. El problema es que estos proveedores externos no diseñaron este tipo de certificados para que se usaran en una red de producción. Los certificados de proveedor preinstalados suelen estar autofirmados o caducados o utilizar claves poco seguras, por lo que los navegadores no confían en ellos. Muchas empresas tienen miles de certificados de proveedor de los que no tienen constancia, certificados que deberían eliminarse y sustituirse por otros que sí se reconozcan como fiables (como mínimo, por certificados TLS/SSL privados). Para optimizar este proceso, conviene utilizar las herramientas de automatización más modernas —como API o URL de ACME—, que facilitan la sustitución y la instalación.

ASEGÚRESE DE QUE LOS SISTEMAS ESTÉN SIEMPRE ACTUALIZADOS

Evitar algunos de los ataques más devastadores de Internet pasa por mantener actualizados los sistemas.

Las revisiones son actualizaciones de los sistemas operativos, servidores, marcos de aplicación, bases de datos y otros sistemas y software que ofrecen protección frente a las vulnerabilidades en un producto (por ejemplo, los sistemas operativos Windows o Linux o los servidores web y equilibradores de carga).

Estas actualizaciones ayudan a prevenir ataques como el error Heartbleed, una vulnerabilidad detectada en la biblioteca de software criptográfico OpenSSL. Todas aquellas personas que, en un momento dado, utilizaron la versión vulnerable del software OpenSSL abrían una puerta trasera que permitía a los atacantes leer la memoria de todos los sistemas que estuvieran protegidos por él. Así, los atacantes podían espiar las comunicaciones o robar datos relativos a los servicios y usuarios.



PROTEJA EL ACCESO A LOS SISTEMAS DE GESTIÓN DE CERTIFICADOS

Adopte herramientas de uso habitual como la autenticación de dos factores y el inicio de sesión único (SSO).

La autenticación de dos factores (2FA), o autenticación multifactor, requiere utilizar más de un método de seguridad para autorizar los inicios de sesión (métodos que suelen ser, bien algo que tenemos, bien algo que sabemos). Proteja sus plataformas de gestión de certificados con un nivel de seguridad adicional para evitar brechas a la hora de administrarlos.

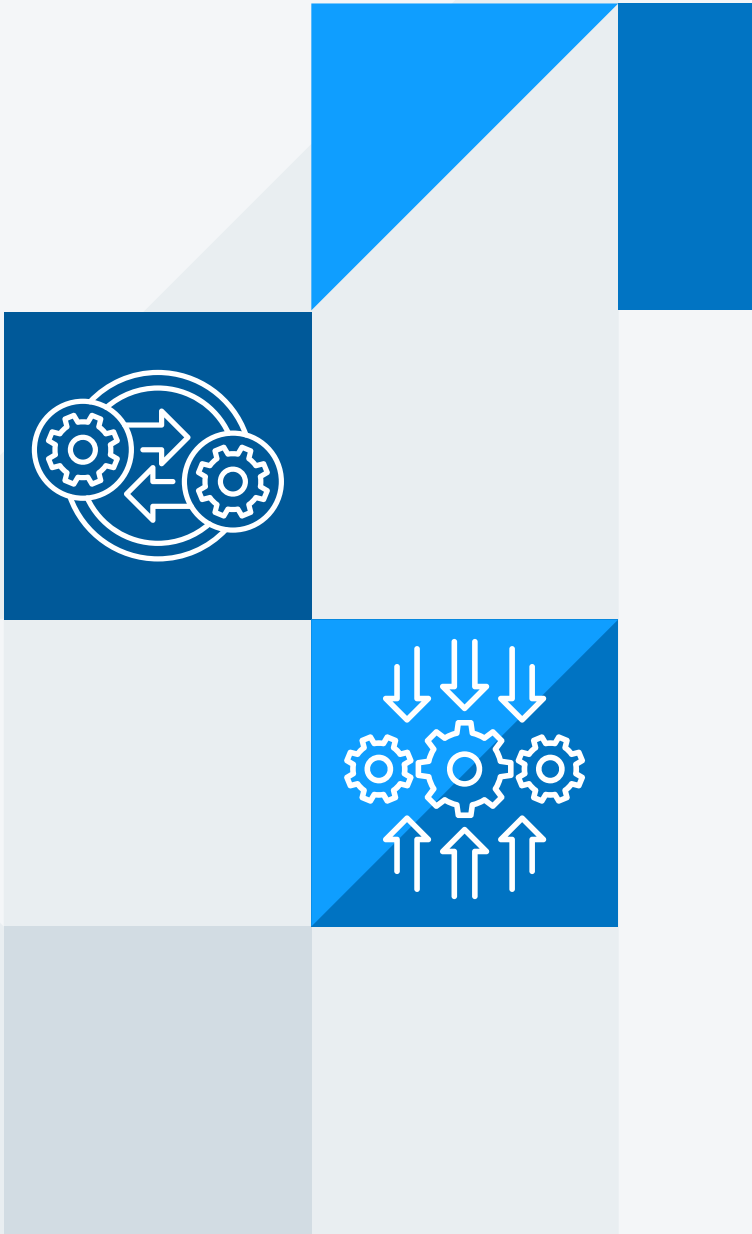
Estos son algunos ejemplos de autenticación de dos factores:

- Autenticación 2FA con dispositivos móviles
- 2FA con aplicaciones de autenticación
- 2FA con generación de tokens

INTEGRACIÓN CON SISTEMAS ITSM

Las plataformas de gestión de certificados se integran con otras soluciones de software como ServiceNow para interactuar sin problemas con las operaciones de TI.

Si dispone de entornos informáticos más complejos, integre su plataforma de gestión de certificados con sistemas de gestión de servicios de tecnologías de la información (ITSM) como ServiceNow para crear los flujos de trabajo de aprobación que se adecúen a los procesos de su empresa. Así, el personal podrá solicitar los certificados TLS que necesite aunque no tenga acceso directo a los sistemas de gestión de certificados. Gestionar los procesos de derivación con un sistema ITSM le permitirá reducir los errores humanos y aumentar el tiempo de actividad.



REVISE LAS ALERTAS POR SI FUERA NECESARIO TOMAR ALGUNA MEDIDA

Benefíciese de paneles que muestran qué elementos es necesario revisar o corregir.

Utilizar un panel centralizado para supervisar el estado de los elementos identificados durante la detección es un primer paso importante, pero también lo es asegurarse de que los datos se presenten de forma clara y detallada y sirvan para tomar las medidas oportunas.

Su sistema de elaboración de informes debería permitirle:

- Ver todos sus certificados desde una única consola.
- Elaborar, descargar, programar e integrar informes detallados.
- Identificar fácilmente elementos sobre los que actuar y problemas concretos, como certificados en los que no se puede confiar, fechas de caducidad próximas y problemas relacionados con el cumplimiento normativo.
- Obtener gráficos y visualizaciones de datos intuitivos que sean fáciles de explicar y presenten un plan de acción claro.

ESTABLEZCA JERARQUÍAS DE NOTIFICACIÓN Y DERIVACIÓN

Defina y automatice los métodos de notificación y sus destinatarios.

Evite que se produzcan brechas de seguridad y que los certificados caduquen estableciendo jerarquías de notificación y derivación. Para cada grupo de certificados, estas jerarquías deberán especificar:

- Cuándo enviar notificaciones
- Por qué medio hacerlo (p. ej., correo electrónico, alertas, Slack, ITSM)
- A qué profesional se entregan
- Umbrales de derivación

Asegúrese también de que las personas con las que deba ponerse en contacto por correo electrónico estén al día con la CA emisora para no perderse ninguna notificación sobre renovaciones o incidentes.

CONFIGURE LOS TIEMPOS DE NOTIFICACIÓN

Defina y automatice las alertas relativas a la renovación para que se envíen 90, 60 o 30 días antes de que caduquen los certificados.

Para evitar que los certificados caduquen, configure el envío de notificaciones en momentos concretos (p. ej., 90, 60 o 30 días antes de la fecha de caducidad). Le recomendamos que renueve los certificados al menos 15 días antes de que caduquen. Así, tendrá tiempo suficiente para realizar las pruebas y verificaciones oportunas. Si su proceso de control de cambios es más largo, es preferible renovar los certificados con 32 días de antelación.

También deben configurarse alertas para los certificados caducados, con plazos similares.

SUPERVISE LOS REGISTROS DE CERTIFICATE TRANSPARENCY

Los navegadores no confiarán en ningún certificado público que no figure en un registro público de Certificate Transparency (CT).

Utilice una herramienta de supervisión de registros de CT para detectar rápidamente certificados en los que no se puede confiar y para identificar y corregir certificados que se hayan emitido a quien no correspondía. Los registros de CT permiten a las autoridades de certificación emisoras de certificados TLS/SSL de confianza saber quién es responsable de estos durante el proceso de validación. Si un tercero emite un certificado para su nombre de dominio (ya sea de forma maliciosa o incumpliendo las políticas), la supervisión de registros de CT lo detecta y le avisa de inmediato.

CONFIGURE ALERTAS DE CAA Y EVITE SOLICITUDES DE CERTIFICADO NO AUTORIZADAS

La autorización de la autoridad de certificación (CAA) es un registro de DNS utilizado para especificar qué autoridades de certificación tienen permiso para emitir certificados para su dominio.

En 2017, el CA/Browser Forum lanzó el proceso de votación Ballot 187, cuyo resultado exige que todas las autoridades de certificación comprueben los registros de DNS CAA y respeten todas las entradas que figuren en él para el dominio en cuestión. El objetivo es dejar que los propietarios del dominio declaren qué autoridades de certificación tienen permiso para emitir un certificado para ese dominio. Gracias a la CAA, también es posible recibir notificaciones si alguien solicita un certificado a una autoridad de certificación no autorizada.

AUTOMATICE LA GESTIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS

Optimice la instalación y renovación de certificados y la generación de CSR.

Cualquier empresa que pretenda gestionar grandes volúmenes de certificados con eficiencia deberá apostar por la automatización. Si la aplica a las diferentes tareas manuales que conlleva la gestión de certificados, podrá minimizar los errores humanos y reducir la cantidad de tiempo y recursos que dedica a gestionar los certificados con periodos de validez más cortos.

La automatización de la gestión de certificados:

- Reduce la carga de trabajo que supone emitir, sustituir y renovar certificados.
- Elimina los errores humanos y evita las configuraciones erróneas para prevenir las interrupciones.
- Aligera el trabajo del servicio técnico gracias al aprovisionamiento automático de usuarios.
- Permite sustituir los certificados en riesgo con eficiencia, lo cual agiliza la corrección.

LOGRE LA AGILIDAD CRIPTOGRÁFICA AUTOMATIZANDO LA GESTIÓN DE CERTIFICADOS

Prepárese para la criptografía poscuántica.

Las empresas que quieran garantizar que sus operaciones resistan el paso del tiempo y cualquier cambio que se produzca en el sector, en general, y en la criptografía, en particular, deberán empezar a utilizar herramientas de automatización desde ya. A largo plazo, automatizar la emisión y renovación de certificados les supondrá un ahorro de tiempo a la hora de gestionarlos, supervisarlos o sustituirlos cuando se produzca algún incidente de seguridad. Además, la automatización también ayuda a actualizar los algoritmos criptográficos para los certificados más fácilmente.

AUTOMATICE LOS PROCESOS EMPRESARIALES

Configure reglas de acceso, flujos de trabajo, plantillas e integraciones.

La automatización de la gestión de certificados va más allá del aprovisionamiento, la instalación y la renovación de certificados TLS sin intervención manual. Automatizando los procesos empresariales se mejora la gestión de la PKI en todo el inventario de certificados y activos criptográficos. Reglas de acceso predefinidas, flujos de trabajo de aprobación y notificación automatizados, inscripción automática, claves seguras, integración con sistemas empresariales... Son muchas las formas en las que la automatización de los procesos empresariales mejora la seguridad y las operaciones.

PERSONALICE LAS INTEGRACIONES GRACIAS A LAS API

Disfrute de una integración directa entre su plataforma de gestión de certificados y los sistemas de la empresa.

Optimice la gestión de certificados con los sistemas empresariales, procesos o productos que ya utilice gracias a la integración de API. Entre las modalidades de integración más comunes se encuentran las integraciones con los sistemas ITSM —para programar las tareas relacionadas con los certificados en función de los procesos ligados a las ventanas de cambio— o con herramientas de detección específicas —para ayudar a conformar una visión unificada del inventario—.

DISFRUTE DE COMPATIBILIDAD ENTRE CERTIFICADOS Y NAVEGADORES EN TODA LA RED

Las raíces de las autoridades de certificación de creación más reciente o de menor tamaño podrían no estar incluidas en los almacenes raíz de ciertos navegadores. Esto supone un problema sobre todo en el caso de los navegadores más antiguos.

Siguiendo las prácticas recomendadas del sector, asegúrese de que los certificados que utiliza en su empresa procedan de una CA consolidada que ofrezca compatibilidad con un gran número de navegadores. Así sabrá que los certificados están incluidos en los almacenes raíz tanto de los navegadores nuevos como de los antiguos, lo que significa que son compatibles con el 99,9 % de las plataformas y los navegadores de los clientes.

No es la primera vez que las raíces de ciertas autoridades de certificación se quedan fuera cuando sale una versión nueva de un navegador. Esto hace que a los internautas les salten mensajes de error cuando visitan los sitios web protegidos por estos certificados, lo cual puede afectar muy negativamente a las tasas de conversión y a la reputación del propietario del sitio web en cuestión.

UTILICE SERVICIOS DE DETECCIÓN E IMPORTACIÓN QUE FUNCIONEN CON CUALQUIER CA

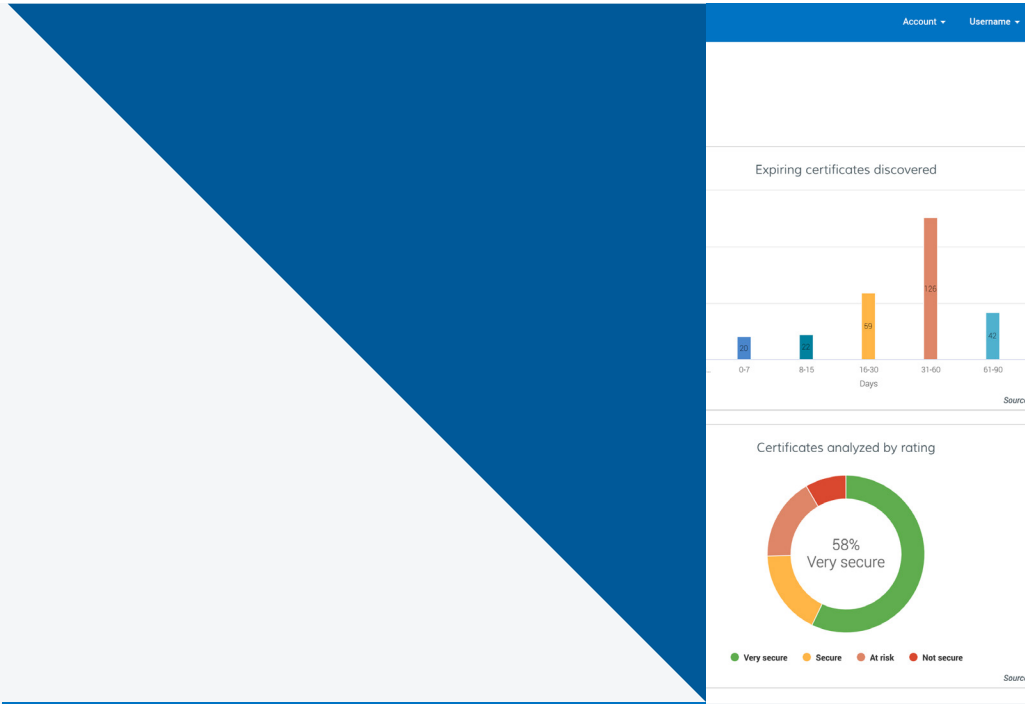
Apueste por una plataforma de gestión compatible con diversos certificados de distintas CA.

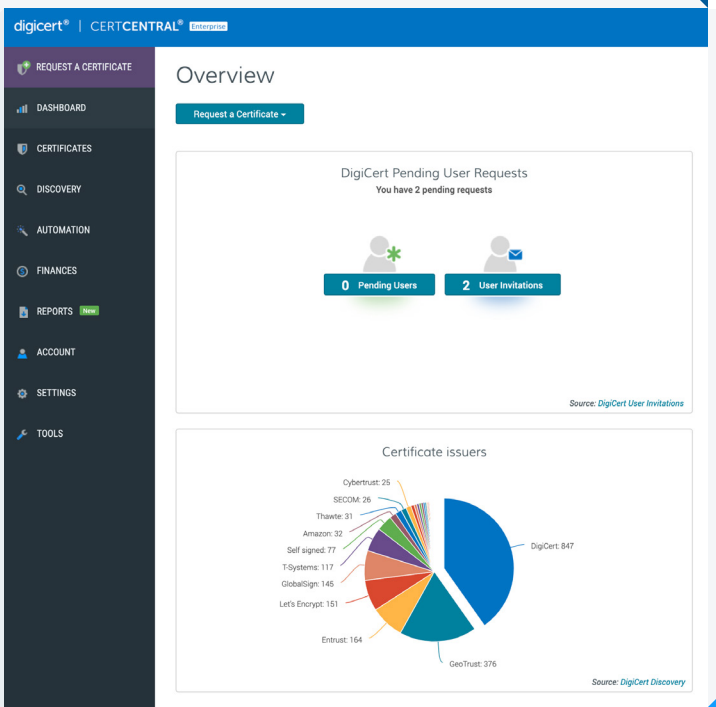
Las plataformas compatibles con cualquier autoridad de certificación le permiten supervisar y gestionar todos los certificados desde una única plataforma, independientemente del tipo que sean y de la CA emisora. Hágase con herramientas de detección que puedan importar certificados raíz privados para realizar tareas de detección a partir de esas raíces o de otros activos criptográficos. Con este enfoque, conseguirá una visión exhaustiva y unificada de todos sus certificados.

CONCLUSIÓN

Ponga fin a las tediosas tareas de gestión del ciclo de vida de los certificados.

Las soluciones de DigiCert le ofrecen todas las funciones que necesita para poner en práctica los cinco pilares de las prácticas de TLS recomendadas: detección, gestión y elaboración de informes, notificación, unificación y —lo más importante— automatización del inventario de certificados. Son intuitivas y completas y constituyen la mejor manera de abordar la gestión de certificados de forma proactiva.





ABORDE LA GESTIÓN DE CERTIFICADOS DE FORMA PROACTIVA

Optimice la gestión del ciclo de vida de los certificados y dedique su tiempo a hacer crecer su negocio. ¿Quiere saber cómo le ayudan los productos de DigiCert a aplicar todas las prácticas recomendadas de gestión de certificados? Escriba a contactus@digicert.com hoy mismo para hablar de sus necesidades en esta materia o visite digicert.com/tls-ssl/certcentral-tls-ssl-manager para solicitar una demostración completa.