Publicado en México el 23/03/2022

#  [Las autoridades de certificación y cómo apoyan a las empresas mexicanas según DigiCert](http://www.notasdeprensa.es)

## Se habla mucho de los certificados TLS/SSL y de su importancia a la hora de proteger los datos de empresas, particulares y gobiernos. Pero solo unas pocas personas entienden el significado de un acrónimo importante que acompaña a los certificados: Autoridades de certificación (CA)

 En las grandes empresas donde hay grandes equipos de TI, depende de los profesionales de la tecnología saber qué hace una CA, pero en las pequeñas y medianas empresas, depende del empresario comprenderlo. Debido a la falta de conocimiento sobre el tema, es muy común que estas empresas se basen en empresas que brindan los certificados digitales gratuitos necesarios para habilitar HTTPS (SSL/TLS) en los sitios web y ahí es donde radica el peligro. Según Roger Werner, Director de CertSuperior, “La idea de tener organizaciones que brinden seguridad SSL gratuita para proteger mejor Internet es noble. Pero en la práctica, al ser organizaciones sin fines de lucro, estas cuentan con pocos recursos y son propensas a cometer errores, lo que para sus usuarios puede resultar bastante costoso. Por esta razón, es fundamental comprar certificados SSL de una Autoridad de Certificación de renombre como DigiCert and #39; and #39;. Según el navegador y el sistema operativo que utilice su empresa, se confía en entre 50 y más de 100 organizaciones diferentes de todo el mundo para garantizar que su experiencia de navegación en Internet sea segura. Estas organizaciones, CA, emiten certificados de autenticación de servidor TLS/SSL. Estos certificados son utilizados por miles de millones de usuarios todos los días para verificar la identidad de los sitios web que visita y para garantizar que cualquier información que envíe a ese sitio web esté encriptada y a salvo de miradas indiscretas. Dada la importancia crítica de esta tarea de proporcionar identidad en Internet, es imperativo que las CA operen bajo un conjunto claro de requisitos para garantizar la seguridad y el cumplimiento. “Las CA en las que los navegadores confían hoy para emitir certificados TLS para sitios web seguros son realmente globales; cada CA tiene la capacidad técnica de emitir un certificado para cualquier sitio web. Desde el punto de vista de la seguridad, cada CA es igual: la seguridad general de Internet es tan fuerte como la CA más débil. Por este motivo, se ha establecido un estándar mínimo para garantizar una base común de seguridad y cumplimiento al que deben adherirse todas las CA” dice Dean Coclin, Director Senior de desarrollo comercial en DigiCert. Los principales navegadores requieren que las CA de confianza operen según las políticas descritas en los requisitos básicos para emitir y administrar certificados de confianza pública del CA/Browser Forum. Estos requisitos están definidos y acordados por un grupo de CA y navegadores y representan un conjunto común de requisitos mínimos para la industria. Garantizar la seguridadUna vez que se acuerdan y finalizan los cambios en los requisitos básicos de CA/Browser Forum, estos cambios se incorporan a los criterios de auditoría utilizados por los auditores para garantizar que las CA se adhieran a los requisitos. Este paso de traducir los cambios de los requisitos básicos en elementos específicos que los auditores verifican durante su compromiso de auditoría es una parte fundamental para garantizar la seguridad y el cumplimiento en la industria. Dado que no hay visibilidad externa de las operaciones y controles internos en una CA, las auditorías periódicas y la experiencia y el conocimiento de los auditores sobre los estándares relevantes juegan un papel importante en la seguridad del ecosistema de certificados. Si algún requisito no está claro o no está completamente definido, diferentes auditores pueden llegar a diferentes interpretaciones de los requisitos. Invertir en seguridad es esencial para las empresas hoy en día. No solo porque protege los datos corporativos, sino que también evita que la información de clientes y proveedores caiga en manos de delincuentes. Un caso de violación de datos puede dañar la reputación de su empresa y costarle mucho más de lo que piensa. Entonces, si desea garantizar una experiencia de navegación segura para su empresa, es esencial invertir en certificados TLS de una CA auditada.

**Datos de contacto:**

Prensa DigiCert Latam

573125893314

Nota de prensa publicada en: [https://www.mexicopress.com.mx/las-autoridades-de-certificacion-y-como-apoyan](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Telecomunicaciones Software Dispositivos móviles



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)