Publicado en Latinoamérica el 27/09/2022

# [Las iniciativas acerca de la confianza digital que están trabajando las empresas según DigiCert](http://www.notasdeprensa.es)

## Diana Jovin, VP de marketing de producto en DigiCert analiza porque es importante que las empresas adopten una política de seguridad de confianza cero. Este enfoque de seguridad de "nunca confiar, siempre verificar" requiere que todos los accesos a redes, aplicaciones y servicios estén autenticados

 Los dispositivos conectados son cada vez más comunes en la vida de las personas y en el funcionamiento de las empresas en todos los sectores de la economía. Las tendencias tecnológicas han cambiado la forma en que los profesionales de TI piensan sobre la seguridad en el perímetro corporativo. Las tecnologías operativas que antes estaban aisladas, como la maquinaria de la planta de producción, los servicios públicos y la infraestructura industrial, los instrumentos hospitalarios o las cocinas industriales, se han vuelto conectadas y vulnerables a los ataques cibernéticos. Las aplicaciones y los servicios se han trasladado a la nube, cambiando los modelos de acceso de los usuarios y pasando a la orquestación bajo demanda, la computación sin servidor y las arquitecturas de datos distribuidos. Los dispositivos han proliferado, y los empleados a menudo conectan sus propios dispositivos personales, desde teléfonos móviles hasta tabletas y computadoras, desde vehículos rastreados hasta redes corporativas. Estos cambios, que desafían colectivamente la noción del perímetro corporativo tradicional, están llevando a las empresas a remodelar los supuestos fundamentales que rigen la seguridad corporativa, de las aplicaciones y de los usuarios. ¿Qué sucede con las aplicaciones y el acceso a TI?Debido a que las empresas ya no pueden confiar en los límites físicos o virtuales para definir qué es confiable o no, muchas organizaciones están adoptando una política de seguridad de confianza cero. Este enfoque de seguridad de "nunca confiar, siempre verificar" requiere que todos los accesos a redes, aplicaciones y servicios estén autenticados. Como resultado, los administradores de acceso e identidad están enfrentando demandas significativamente mayores en sus organizaciones: Más puntos de acceso que necesitan autenticación Mayor volumen de autenticaciones Aumento de los tipos de autenticación (p. ej., autenticación biométrica o sin contraseña) Administración de identidad, integridad y encriptaciónEn un entorno sin perímetro, la cantidad y los tipos de cosas que deben asegurarse también aumentan. El rol del administrador de PKI se ha expandido más allá de la seguridad web TLS tradicional para presentar casos de uso nuevos y en expansión en toda la organización: Identidades de servidores, usuarios de dispositivos Ampliación de métodos de autenticación e inscripción Integridad de firmas digitales, documentos, contenido y software, con pistas de auditoría para remediación Comunicación segura y encriptada Correo electrónico seguro Estos casos de uso de PKI proliferan al mismo tiempo que se reducen los períodos de validez de los certificados para la confianza pública. Si bien los períodos de validez más cortos aumentan la seguridad de los certificados, los turnos más rápidos aumentan la carga administrativa de la gestión, así como el área de superficie de riesgo de interrupción del negocio. No es sorprendente que esto esté impulsando una mayor necesidad y atención por las soluciones de gestión de PKI que ayuden con la gobernanza de este panorama de PKI en expansión. Dispositivos conectados más segurosLos dispositivos conectados, ya sean dispositivos personales que se conectan a una red o tecnología operativa que se conecta, aumentan el área de superficie de ataque que ahora debe protegerse. Los administradores de seguridad de tecnología operativa y de red no solo deben considerar cómo aprovisionar la identidad del dispositivo, sino también cómo proteger los dispositivos en funcionamiento: cómo hacer que los dispositivos sean más resistentes a la manipulación, cómo asegurar la comunicación entre ellos, cómo gobernar cómo se conectan a la red. , cómo unir los dispositivos heredados (brownfield) y nuevos (greenfield) y habilitar la autenticación mutua entre ellos, cómo monitorear las amenazas. Los directores de productos de seguridad que definen y crean soluciones centradas en dispositivos, a su vez, deben considerar el área de superficie que debe protegerse durante todo el ciclo de vida del dispositivo (entre fabricantes de chips, fabricantes de dispositivos, desarrolladores de aplicaciones, operadores de dispositivos y usuarios de dispositivos) durante toda la vida. del dispositivo El modelo de seguridad para la organización sin perímetroLos componentes básicos de la confianza digital (estándares, cumplimiento y operaciones, administración de confianza y confianza conectada) son la tecnología fundamental que permite a las empresas operar de forma segura en un mundo en el que un límite corporativo ya no define qué es de confianza y lo que no lo es. Las soluciones de confianza digital permiten a las empresas: Administrar identidadesProporcionar identidades confiables a usuarios, dispositivos, servidores y otros recursos de TI para respaldar las necesidades de autenticación de usuarios, redes y dispositivos Administrar y automatizar ciclos de vida de certificados y acceder a flujos de trabajo para respaldar las crecientes demandas de TI y reducir los errores humanos Administrar la integridadGobierne la integridad y el no repudio de firmas, documentos y contenido Establezca la integridad del software y amplíe la confianza del software a los usuarios intermedios y en todas las operaciones de la red y la nube Conexiones y operacionesComunicación segura de usuario y de máquina a máquina Ciclos de vida seguros de los dispositivos para un funcionamiento confiable y capacidad de actualización Monitoreo y remediar vulnerabilidadesSupervisar continuamente los activos criptográficos dentro del entorno corporativo e identificar y remediar vulnerabilidades. Las iniciativas de confianza digital en toda la empresa pueden establecer un enfoque integral y unificado de la seguridad dentro de una organización sin perímetro, abordando la forma en que la desintegración del perímetro corporativo tradicional está dando forma a las demandas de seguridad dentro de los diferentes departamentos de TI.

**Datos de contacto:**

DigiCert Latam

3125893314

Nota de prensa publicada en: [https://www.mexicopress.com.mx/las-iniciativas-acerca-de-la-confianza-digital](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Internacional E-Commerce Software Ciberseguridad Dispositivos móviles



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