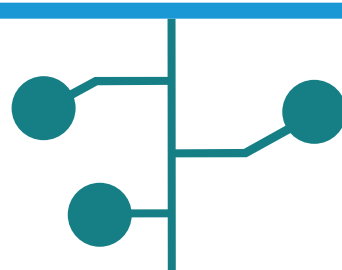


# EXTENSIONES DE SEGURIDAD DEL SISTEMA DE NOMBRES DE DOMINIO

## AYÚDANOS A PROTEGER LA INFORMACIÓN DEL DNS QUE ENVÍAS POR INTERNET



Las Extensiones de Seguridad del Sistema de Nombres de Dominio (DNSSEC) permiten que los registratarios **firmen digitalmente** la información que ingresan al Sistema de Nombres de Dominio (DNS). De esta manera, los consumidores están protegidos, dado que no reciben datos del DNS que hayan sido dañados en forma intencional o accidental.



### LÍNEA DE TIEMPO



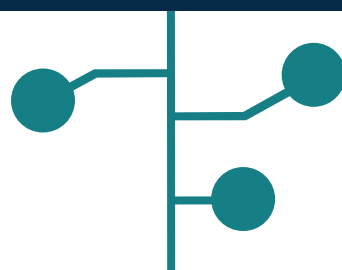
1980

Cuando se diseñó el DNS, la seguridad no fue un aspecto central. Los atacantes podían **interceptar los mensajes enviados en el DNS y desviarlos hacia otro destino en Internet en lugar del destino** indicado por el emisor del mensaje.



1990

La comunidad técnica del DNS diseñó una solución definitiva para este problema: las DNSSEC. Las DNSSEC refuerzan la autenticación del DNS mediante firmas digitales basadas en **cifrado de clave pública**.



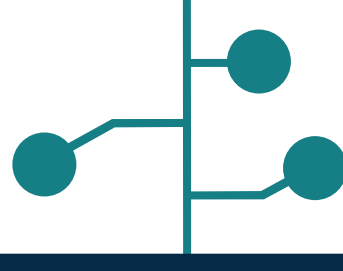
### LAS DNSSEC EN ACCIÓN



**Para que las DNSSEC funcionen, sus dos componentes deben estar habilitados.**

Los registratarios, responsables de publicar información en el DNS, deben **asegurarse de que sus datos en el DNS estén firmados con DNSSEC**.

Los operadores de redes necesitan **habilitar la validación de DNSSEC en los resolutores** que procesan las búsquedas de los usuarios en el DNS.



### BENEFICIOS DE IMPLEMENTAR LAS DNSSEC



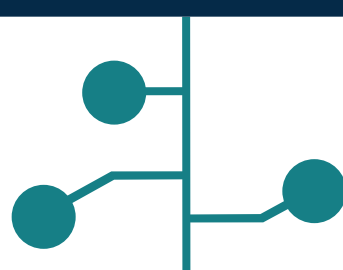
Ayudan a proteger la Internet, los usuarios finales, las empresas, las organizaciones y los gobiernos.



Reducen las vulnerabilidades a los ataques.



Promueven la innovación. Las DNSSEC verifican y protegen los datos del DNS; como resultado, los datos son confiables en aplicaciones externas al DNS.



INVITA A TUS OPERADORES DE REDES A QUE HABILITEN LAS DNSSEC



ICANN

PARA MÁS INFORMACIÓN SOBRE LAS DNSSEC, VISITA:

<http://go.icann.org/OCTOpublications>

<http://go.icann.org/DNSSEC>