1. **Evidenciar que las aplicaciones Web y Apps sean evaluadas a través de un análisis de vulnerabilidades y pruebas de penetración.(Informes de pruebas realizadas y planes de remediación)**

Actualmente no contamos con dichos informes, sin embargo, se tiene planificado contratar un proveedor de seguridad informática que evaluará constantemente las vulnerabilidades de nuestros sistemas, presentando informes de manera frecuente para realizar y ejecutar los planes de remediación de ataques informáticos.

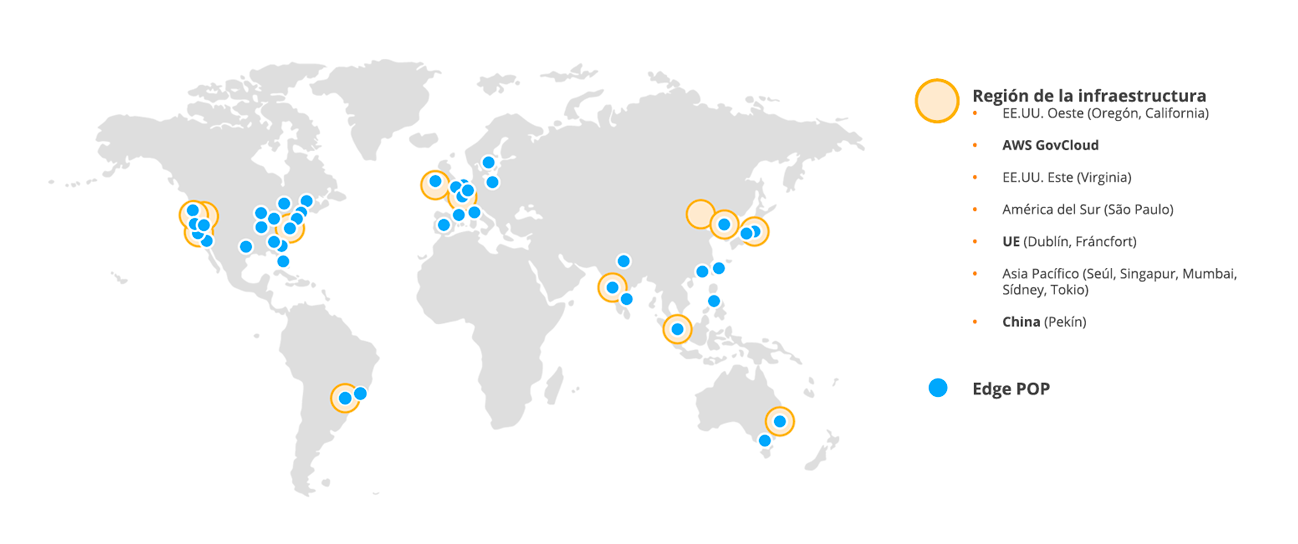
1. **Evidenciar controles de seguridad que tienen implementado la plataforma Web y Apps de ser el caso para proteger la información (Uso de certificados) y controles en el login.**

Los servicios web con los que interactúan nuestros aplicativos cuentan con controles de seguridad y de autenticación basados en JWT (Json Web Tokens) el cual permite brindar seguridad a nuestras aplicaciones.

Adicionalmente, nuestros aplicativos permiten la integración con Active Directory para facilitar y asegurar la autenticidad en el acceso.º

1. **Precisar lugar y país donde se almacena la información. (Flujos transfronterizos).**

El proveedor cloud Amazon tiene servidores a nivel mundial, el cual garantiza la alta disponibilidad, en nuestro caso el data center principal en el cual se alojará nuestra información estará en la zona Oeste de EE.UU.



1. **Brindar tiempo de almacenamiento y medios usados para compartir la información almacenada. (listar medios seguros)**

La información general estará en los servidores de nuestro proveedor Amazon, el cual garantiza el respaldo de la información en tiempo real. Otro tipo de almacenamiento, ya sean Back Ups en medios físicos y el tiempo de respaldo dependerán de los requerimientos del cliente, en este caso El Banco Financiero.