SEGURIDAD EN LA NUBE

FUNDAMENTOS DE NUBE

La <<nube computacional>> es un conjunto de tecnología que permite acceder remotamente en cualquier momento, a variados recursos, servicios, programas e información, sin la necesidad de contar con un servidor físico local o propio. De las cuales podemos encontrar en estas tres modalidades: nube pública, nube privada y nube hibrida.

La <<nube informática>> es un conjunto de servicios en línea en la cual podemos categorizar en estos tres servicios: Infraestructura como servicio (IaaS, por su s siglas en ingles), plataforma como servicio (PaaS, por su s siglas en ingles) y software como servicio (SaaS, por su s siglas en ingles).

ASPECTOS GENERALES DE SEGURIDAD

Se debe considerar algunos aspectos generales de seguridad al momento del uso de un servicio en nube. En la que podemos agrupar en los siguientes puntos:

1- ENTENDER TUS RESPONSABILIDADES:

Revisar las condiciones y políticas de uso del servicio que se está adquiriendo, si cumple con las necesidades y el alcance de responsabilidad de las partes involucradas.

2- CONTROLES DE ACCESO:

Conocer los controles de usuario y credenciales de acceso hacia los servicios. Conocer los controles de segregación de la red, servicio y su aislamiento. Conocer que el canal administrativo o soporte a la aplicación es distinta al de la producción.

3- CONTROLES PARA LA MITIGACIÓN DE RIESGOS:

Siempre es recomendado contar con servicios adicionales de seguridad para la mitigación de riesgos. Ejemplo de servicios de protección perimetrales como firewall de última generación (NGFW, por sus siglas en ingles), DNSSEC, WAF, Anti-Spam, anti-virus, etc.

4- ACTUALIZACIÓN DE SISTEMAS:

Es importante tener las actualizaciones de los sistemas ya sea hardware por el proveedor de nube y del software por el cliente, para la mitigación de riesgos de forma integral.

5- PROTECCIÓN DE DATOS:

Revisar la capacidad de contar con respaldo de la información y revisar que estos estén funcionales en caso de requerir una restauración. También contar con el cifrado de datos para la mitigación del riesgo de la fuga de información. Y considerar los aspectos legales de la protección de datos como su legislación. En Panamá se cuenta con la ley 81 de 2019 sobre la protección de datos personales.

CSIRT
EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

E-Mail: info@cert.pa
Phone: +507 520-2378
Web: https://cert.pa
Twitter: @CSIRTPanama