Seguridad Comunicaciones Quakki

El control de acceso a los centros de datos de Quakki se lleva conjuntamente con AWS nuestro proveedor de Cloud Computing. Esta asociación nos proveé de Data Centers con la máxima seguridad disponible en el mercado, con continuos chequeos y mantenimientos para que nuestra información esté segura las 24 horas con independencia de cualquier accidente que pueda suceder. Con infraestucturas repartidas alrededor del mundo y personal de mantenimiento, monitorización y seguridad especializado y listo para responder antes cualquier eventualidad.
Nuestro proveedor de Cloud Computing AWS admite 89 estándares de seguridad y certificaciones de conformidad entre las que incluyen PCI-DSS, HIPAA/HITECH, FedRAMPP, RGPD, FIPS 140-2 y NIST 800-171.

Añadimos otra capa de cifrado a nuestros datos en reposo usando algoritmos de cifrado de alto nivel, como parte de una estragegia de segudidad de defensa en profundidad, dicho algoritmo es utilizado por instituciones del calibre de la americana N.S.A.
https://us-cert.cisa.gov/bsi/articles/knowledge/principles/defense-in-depth

Hemos diseñado e implementado una red Privada dentro de los centros de datos de los cuales nos provee AWS. Esta zona dispone de diversos controles de seguridad basados en el principio de menor privilegio e incluye varias capas de control basado en los modelos de ACL de AWS. Las instancias de esta red tienen un uso restringido de todo el tráfico entrante y saliente salvo excepciones estrictamente controladas y monitorizadas por nuestro equipo de sistemas. Nuestra red cumple con las normativas R.G.P.D. vigentes para los estados de la UU.EE.

Todos los datos de las comunicaciones Quakki que fluyen en la red privada se cifran de manera automática en la capa física antes dejar sus instalaciones protegidas.

Todo el tráfico de las interconexiones entre clientesrecibe 5 capas de cifrado y verificación de identidad. En estos podemos distinguir el cifrando de las sesiones, codificación de los datos, codificación de los datagramas necesarios para la comunicación, verificado de los datos para la conexión handshake, comprobación de origen de los datos recibidos, etc.

La seguridad para los sistemas que hacen posible las comunicaciones, se ven beneficiados de todas las certificaciones, seguridad y programas de conformidad de los sistemas AWS. Las cuales podemos ver en:

https://aws.amazon.com/es/compliance/services-in-scope/
https://aws.amazon.com/es/compliance/programs/

Disponemos de una seguridad mejorada con la cual monitoreamos y verificamos continuamente el hardware y el firmware de la instancia. La virtualización de los recursos se descargan mediante distintos hardware y software dedicados, lo que minimiza la posible superficie de ataques. Además, el modelo de seguridad de Nitro System está virtualmente bloqueado y prohíbe el acceso administrativo, lo que minimiza o directamente elimina la posibilidad de errores humanos o alteraciones.

El acceso a las instancias utiliza la criptografía de clave pública para cifrar las distintas contraseñas y, además, el nuestros servidores utilizan una clave privada para descifrar dicha clave evitando el acceso de usuarios sin privilegios.

Además debemos puntualizar que nuestros servidores funcionan sobre distribuciones linux las cuales reciben mantenimientos periódicos. Estos servidores siempre están actualizados con los últimos parches de seguridad disponibles que son continuamente probados y chequeados además de realizar una monitorización sobre estos para detectar cualquier incidencia o cualquier variación en el uso normal de los mismos.

Nuestros servidores además disponen de firewalls actualizados y monitorizados que mantienen un control sobre los puertos abiertos de los que disponen nuestros servidores con una configuración que se adecua a las necesidades de los productos sin perder la vista la seguridad.