Equipo 9:

* Stefany Salamanca
* Lara Converso
* Andres Felipe Monterrosa
* Santiago Duran
* Jorge Andres Jimenez
* Maria Eugenia Gadea

**Micro-desafío**

**1. Utilizando el documento de presentación de la actividad, cada mesa deberá**

**colocar el link al documento del plan de seguridad diseñado en la actividad**

**anterior, para que otro grupo pueda acceder y analizarlo.**

**2. Realizar una auditoría del plan de seguridad de uno de los grupos en base a**

**los escenarios planteados.**

**3. Buscar vulnerabilidades y fallas que faltaron solventar. Cuando se encuentre**

**una falla, hay que explicar por qué es una vulnerabilidad y cómo podríamos**

**atacar. A su vez, se debe explicar cómo solucionar dicha vulnerabilidad.**

**link:**[**https://docs.google.com/document/d/1LpvR0Zf\_r5I7rNB-KXtjZ0lL2GLzL0PBgWl3XZzbkl8/edit**](https://docs.google.com/document/d/1LpvR0Zf_r5I7rNB-KXtjZ0lL2GLzL0PBgWl3XZzbkl8/edit)

Análisis del plan de seguridad:

El plan propuesto cubre la mayoría de la vulnerabilidades, pero creemos se podrían realizar las siguientes acciones para mejorarlo:

* Concientizar acerca de la importancia de mejorar la infraestructura y la seguridad física , pues de nada sirve tener distintos tipos de servidores si estos pueden verse afectados por problemas de falta de electricidad / bajos recursos, esto puede resolverse, por ejemplo, instalando una UPS.
* Es muy importante crear directivas para restringir ciertas actividades no deseadas o peligrosas en los trabajadores, se puede implementar una conexión segura y privada por medio de una VPN ya que los colaboradores están de manera remota.