**Grupo 2:**

**Lo primero que deberían hacer en la parte física es ponerle un UPS en cada dispositivo de la empresa, hacer un sistema de respaldo de datos y un sistema redundante para no perder la información en ningún caso, aparte realizar constantes copias de seguridad diarias, semanales y mensuales, hacer copias de los datos de mayor importancia cada vez. Para mejorar la seguridad on site instalaremos Pararrayos, extintores, detectores de humo para la protección de los equipos y alarma contra intrusos además de cámaras.**

**Además deberíamos tener antivirus de calidad, firewall, cifrado de datos y control de acceso en cada uno de los dispositivos, no escatimar en los gastos de estos programas, mejorar la seguridad de la página web para evitar el ataque de hackers y el robo de datos.**

**Finalmente hacer una entrevista con cada empleado para conocer las razones de su resistencia al cambio de seguridad, si es una cuestión de miedo al desconocimiento o hay una brecha de seguridad que no quieran cerrar.**

**Integrantes:**

* **Nacho Colazo**
* **Ramon Colmenares**
* **Nahuel Muñiz**
* **Daiana Manelli**

**Mesa 3 - Auditoría del plan de Seguridad :**

**Un UPS por máquina parece excesivo en cuestión de espacio físico, pondríamos un UPS que pueda tener varios computadoras conectadas en simultáneo.**

**En vez que entrevistas personales con los empleados que llevarían mucho tiempo y apelan a la individualidad, generaríamos grupos de trabajo donde realizar explicaciones de forma didáctica con personal calificado.**