Equipo 2

* Gabriella Gozzerino Taboada
* Lucia María Yanicelli
* Natalia Narvaez
* Romina Colombo

1. Hacer un análisis de la situación actual de cada empresa que nos toque.
2. Para cada escenario planteado, crear un plan de seguridad
3. Este plan debe ser de 6 pasos e incluir, seguridad lógica, física, pasiva, activa y controles de medida de seguridad, y de vulnerabilidades que podrían explotar los atacantes

Empresa ya consolidada que se dedica a brindar servicios informáticos, la mayoría de sus empleados trabajan en remoto, pero hay algunos que van on site, necesitan una intranet más segura, y la información confidencial de la empresa tiene buena seguridad lógica pero muy poca física, aunque igualmente desean tener asesoramiento en seguridad lógica, no tienen problemas en invertir dinero, pero sus empleados se resisten al cambio de nuevas restricciones. Poseen una página web donde brindan sus servicios y los clientes pueden contactarse a través de la misma.

### ESCENARIO 1: Intranet más segura

Luego de realizadas las entrevistas con los empleados llegamos a la conclusión de que, si bien la empresa posee recursos que ayudan a que la intranet sea más segura, los empleados no saben utilizarla y, aquellos que sí, no lo hacen con mucha frecuencia.

**Paso 1:** Capacitar a los empleados (Medida de protección proactiva directiva)

**Paso 2:** Instalar una VPN

**Paso 3**: Adquirir un UPS para el servidor de la empresa (Seguridad Física)

**Paso 4:** Realizar un respaldo datos y sistema redundantes (Seguridad Física)

**Paso 5:** Establecer un control de acceso a la intranet, fijando características mínimas de contraseña para aumentar la seguridad (Seguridad Lógica)

**Paso 6**: Invertir en un antivirus combinado con un firewall de software para evitar que malwares roben información confidencial de la empresa (Seguridad Lógica)