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)

Para empezar a poner en práctica los conocimientos adquiridos, necesitarás realizar la siguiente actividad.

1. En los cuadros de grupo, colocar el link al documento del plan de seguridad diseñado en la actividad anterior, para que el 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 porque es una vulnerabilidad y como podriamos atacar, a su vez explicar como solucionar la vulnerabilidad.

El nivel de seguridad de la empresa no es para nada bueno, no tienen backups por si llegan a tener inconvenientes con la información, sumándole gravedad tampoco tienen privacidad de la información sensible que tiene, lo que provoca que además de que están completamente desvalidos contra cualquier tipo de secuestro de información y haría los ataques más específicos en la información objetivo, además no podrían rastrear quien realizó el ataque porque TODOS pueden ver la info.

* Establecer una red Proxy para limitar el envío de información desde la organización.
* Capacitación de ingeniería social para aquellos que no tienen conocimientos en informática.
* Uso de una Nube para tener una copia de seguridad, esta opción es más asequible que tener un almacenamiento físico
* Limitar el uso de puertos USB’s.
* Añadir antivirus y un firewall.
* Cifrar la información de la base de datos que contiene la información de los clientes.
* Crear sistemas de roles para jerarquizar el acceso a la información.

**Vulnerabilidades/Mejoras:**

La copia de seguridad la haríamos también física con un respaldo de datos y sistemas redundantes.