## -Grupo 5

### Escenarios para grupos 1, 3, 5, 7, 9, 11

- Empresa emergente dedicada a la venta de productos fertilizantes para campos con una capacidad financiera acotada. Todos sus empleados trabajan on site y están dispuestos a recibir capacitación. Poseen actualmente dos personas encargadas de sistemas, las cuales manejan información sensible, pero que todos los usuarios pueden ver (no es política de la empresa). No realizan copias de información porque no las creen convenientes. Poseen una página web donde hay catálogos y los clientes pueden hacer compras a través de la misma.

## Microdesafío 📌

La empresa que se les haya asignado los contrata como asesores de seguridad, ya que creen que es una parte fundamental para resguardar sus activos. En base a lo visto en clase y clases anteriores deben hacer:

1. Un análisis de la situación actual de cada empresa que se les haya asignado.

   La información sensible de la empresa puede ser vista por todos los usuarios, a pesar de no ser esto una política de la empresa. No se realizan copias de seguridad de la información. La información de los clientes, que suministran a la hora de hacer compras en la página web, podría estar en riesgo.

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.

**PLAN DE SEGURIDAD**

**Seguridad Lógica:** Control de acceso podría ser para una parte de la información se mantenga privada únicamente por las personas encargadas de sistemas de la empresa, en conjunto del Cifrado de datos.

**Seguridad Física:** Respaldo de datos, haciendo copias de seguridad periódicas de la información. Conexión de equipos a una ups. Contar con extintores, detectores de humo y alarma contra intrusos.

**Seguridad pasiva:** análisis y búsqueda de potenciales ataques que puede estar expuesta la página web de la empresa y la información que a través de ella se transa, como los datos de pagos de los clientes.

**Seguridad activa:** Recomendamos a la empresa, que tengan buenas prácticas para poder evitar cualquier posible inconveniente, como uso y empleo adecuado de contraseñas, uso de software de seguridad informática, como antivirus, antiespías y cortafuegos, y encriptar los datos importantes.

**Controles de medida de seguridad:** haremos hincapié en las medidas proactivas, principalmente en las preventivas, las cuales buscan que no se produzca un accidente o cualquier tipo de acción indebida en los sistemas.