****

**Práctica de diseño de plan de seguridad**

**Práctica integradora**

# **Objetivo**

Se dividirá a los estudiantes en 10 grupos

# **Microdesafío**

Para empezar a poner en práctica los conocimientos adquiridos, necesitarás realizar la siguiente actividad. La empresa que les toque 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. 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

Esta serie de pasos y sugerencias, deben ser puestas en un documento que pueda ser compartido con otras personas, especificando el grupo que son y el escenario que les tocó.

Escenarios para grupos - 1, 3, 5, 7, 9

* Empresa emergente dedicada a la venta de productos fertilizantes para campos, con una capacidad financiera acotada, todos sus empleados trabajan on site y están dispuesto 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.
  + - 1. Estado

A continuación presentamos el estado de la empresa auditada:

* La empresa está dispuesta a implementar medidas de seguridad preventivas
* No se está protegiendo la confidencialidad de información sensible
* No se está protegiendo la disponibilidad de información sensible
* No se está protegiendo la disponibilidad y confidencialidad de la información de ventas

2 y 3. Plan de seguridad

* La empresa está dispuesta a implementar medidas de seguridad preventivas: Realizar y diseñar capacitaciones que abarquen los temas (según corresponda): Importancia de cifrado de datos, respaldo de datos, sistemas redundantes, control de acceso, antivirus, firewall.
* No se está protegiendo la confidencialidad de información sensible: Implementar seguridad lógica que proteja la confidencialidad aplicando control de acceso, cifrado de datos, aplicar antivirus y firewalls.
* No se está protegiendo la disponibilidad de información sensible: Al ser información sensible, sinónimo de importante y de acceso limitado, se recomienda realizar un respaldo de datos (backup de la información) y generar un sistema redundante (copia de la información más importante), para asegurar la disponibilidad de la información.
* No se está protegiendo la disponibilidad y confidencialidad de la información de ventas: Teniendo en cuenta que se maneja información de ventas que podría incluir precios e inventarios, se recomienda realizar auditorías en periodos de tiempo que la empresa considere prudente para así evaluar la eficiencia, gestión de recursos, y normativas; control de versiones, y detección de intrusos. Por otro lado, para asegurar la disponibilidad recomendamos aplicar respaldo de datos y sistemas redundantes.