

Práctica de diseño de plan de seguridad

# Práctica integradora

## Objetivo

Para empezar a poner en práctica los conocimientos adquiridos, realizaremos la siguiente actividad. Se crearán grupos, divididos en sus respectivas salas y realizarán la siguiente ejercitación.

## 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.
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 debe ser presentada en un documento que pueda ser compartido con otras personas, especificando el grupo que son y el escenario que les tocó.

Escenario para grupos 2, 4, 6, 8, 10, 12

* Empresa ya consolidada que se dedica a brindar servicios informáticos. La mayoría de sus empleados trabajan de forma remota, pero hay algunos que lo hacen on site. Necesitan una intranet más segura. 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.

**ANALISIS**

La empresa ya cuenta con algunas cosas pero se necesita garantizar la seguridad mediante una VPN, asegurar la actualización de sus sistemas informáticos y empezar a capacitar al personal interno para el aseguramiento de la información, mejores prácticas en el uso del software y en la confidencialidad de la información.

En su datacenter ser necesita mejorar la conexión física mediante UPS y potenciar los hardware de los equipos de cómputo, también podría optarse por la creación de un cuarto frio para las máquinas y para que su vida útil aumente.

**PLAN DE SEGURIDAD**

* A nivel lógico: Se debe realizar mejoras al antivirus, adquisición de una VPN y software para cifrar los usuarios de los empleados.
* A nivel físico: Adquisición de sistemas balanceadores para asegurar la persistencia del sistema, y garantizar los respaldos de la información en la nube., también en cintas. Mejorar la parte eléctrica de la empresa mediante UPS, sobre todo en la parte de los servidores.
* A nivel Activo: Comprar un servidor dedicado a mejorar la seguridad de la VPN, mejorar la seguridad con un antivirus fuerte de pago, realizar la encriptación de los usuarios y password de los usuarios con algún asistente de inicios de sesión y hacer uso de office 365 como una extranet para el uso compartido de datos y archivos. Para la conexión interna se sugiere el uso de un proxy como fortinet.
* A nivel pasivo: Charlas sobre seguridad informática, correos internos informativos sobre la prevención de phishing y el spam, sugerencias del buen uso de las copias de seguridad y el aviso oportuno al equipo de seguridad informática.
* A nivel de vulnerabilidades: Crear un equipo encargado de hacer hacking ético dentro de la compañía y este en constantes campañas de seguridad verificando cuales serían las vías por las que atacarían desde afuera a la empresa.
* A nivel de controles de seguridad: Para este caso, ayudar al acceso de los usuarios al software de la empresa mediante autenticaciones en 2 pasos y token con duración de tiempo, también que solo se pueda acceder mediante passwords seguros y usuarios calificados de la empresa.