



Certified Tech Developer

The Ultimate Degree

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.

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 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.



Equipo 5:

Seguridad Lógica: Crear un control de acceso (usuario y contraseña), cifrado de datos.

Seguridad Física: Crear un respaldo de datos. Utilizar un UPS y realizar un respaldo de datos. Ademas deberán utilizar sistemas redundantes

Seguridad Pasiva: Realizar varias copias de seguridad.

Seguridad Activa: Usar software de seguridad: como antivirus, antiespías, cortafuegos.

Controles de medida de seguridad: Acceso a la oficina solo al personal autorizado.

Vulnerabilidades: Todas las copias de seguridad están en un solo servidor. Además la capacitación de los empleados fue poca.

ANOTACIONES MESA 4:

Vulnerabilidades detectadas:

Por falta de un sistema redundante, si falla el servidor podrían comprometerse todas las copias de seguridad. Es importante aumentar la

capacitación que se brinda a los empleados para que aprendan a manejar nociones básicas de seguridad.

Si la página web no tiene medidas de seguridad como certificados SSL; terceros podrían obtener información de los clientes que compran en la página web.

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

- 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.