**Integrantes:**

* Mateo Adan
* Estefani Gonzalez
* Stepahania Martheyn
* Lorena Pérez
* Marcela Ramírez
* Melisa Saldarriaga

**Texto**

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.

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:

**Preguntas**

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

**Rt//** Actualmente se encuentra con que la empresa presenta falencias en la seguridad física y por ende, teniendo en cuenta que no todos los empleados se encuentran en el sitio de trabajo, se debe de considerar las mejoras en esta área primordialmente para evitar la vulnerabilidad en ese ámbito

**2.** Para cada escenario planteado, crear un plan de seguridad

Identificar que vale la pena proteger, este paso inicial implica averiguar el conjunto de los activos de la organización, incluido el personal, el hardware, software, sistemas y datos que componen tu sistema informático. Pueden incluir programas informáticos, servidores y servicios externos como alojamiento web, además de evaluar riesgos estableciendo qué es lo que podría poner en peligro los activos anteriores, una vez que se evalúa el daño potencial de cada amenaza y la probabilidad de que se produzca, se decide qué amenazas son las más importante e interesantes para empezar a proteger, por último se debe restringir el acceso al servidor o instalar firewall de hardware.

**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.

**Rt//**

* **Seguridad Física:** implementaremos mecanismos de prevención (control de acceso a los recursos) y de detección (si un mecanismo de prevención falla o no existe debemos al menos detectar los accesos no autorizados cuanto antes). Implementar un UPS para posibles problemas con el suplemento de energía, hacer backups regularmente de los datos almacenados de los clientes. En el área de servidores tener elementos como extintores, alarma contra intrusos y pararrayos.
* **Seguridad lógica:** Asegurar la implementación del antivirus y los Firewalls buscando que los datos que se compartan entre los diferentes equipos no presenten fallas que generen pérdidas de información, además de que se requiere el control de los accesos con la intención de que solo el personal de la empresa pueda acceder a los equipos y claramente a la información.
* **Seguridad Activa:** Emplear contraseñas seguras, encriptar los datos importantes, actualizar el antivirus, realizar copias de seguridad, Correr antivirus periódicamente.
* **Seguridad pasiva:** Se encuentra como medida de gran utilidad que se comience a implementar las copias de seguridad en servidores externos, buscando salvaguardar la información en caso de inconvenientes en el on site o ataques a la red interna de la organización.

* **Controles de medida de seguridad:** Involucrar a toda la empresa en la seguridad y monitorear continuamente para dar una respuesta inmediata en caso de un ataque. Se puede hacer una guía para controlar que deben o no hacer los empleados, ante comportamientos sospechosos prevenir su ejecución haciendo que se visualice advertencias .

Se puede contar con un hacker white hats, que esté al tanto de los movimientos que se generen en la organización y contar con las acciones pertinentes antes de tener fallos, corrigiendo posibles “huecos” que comprometan la integridad del sistema, tras haber detectado los posibles ataques.