**Actividad Clase 25**
**Grupo N°10**

**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.

**Desafío:**
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 medidas de seguridad y de vulnerabilidades que podrían explotar los atacantes.

**Respuestas:**

**Situación actual de la empresa:**

- Seguridad física deficiente.
- Buena seguridad lógica pero puede mejorar.
- Necesitan una intranet más segura.
- Dispuestos a invertir en un plan de seguridad adecuado.
- Resistencia a nuevas restricciones por parte de los empleados.

**Plan de seguridad:**

**Paso 1:** Identificar los bienes, datos e información sensible que se desea resguardar.

**Paso 2:** Llevar un registro de situaciones de seguridad informática que se hayan presentado con anterioridad, para así planificar y analizar el tipo de riesgo al cual se puede encontrar expuesto de una manera más frecuente.

**Paso 3:** Llevar un registro de aquellas eventualidades que se han presentado por error del personal en el ámbito informático, lo cual puede ayudar a corregirlas de manera oportuna.

**Paso 4:** Establecer prioridades de seguridad informática, es decir, decir que debe establecerse un orden de riesgo, al momento de atender una amenaza o ataque que pueda presentarse.

**Paso 5:** Una vez presentada la eventualidad o amenaza debe aplicarse lo siguiente:

**Para mejorar la seguridad activa:**

- Uso y empleo adecuado de contraseñas mediante combinaciones de letras, números, mayúsculas y otros caracteres.
- Uso de software de seguridad informática, como antivirus, antiespías y cortafuegos.
- Encriptar los datos importantes: cifrar los datos o la información mediante un algoritmo de cifrado con una clave para que el dato/información sólo pueda ser leído si se conoce la clave de cifrado.
- Instalar un certificado de seguridad en la página web para que los datos que envían los clientes viajen cifrados y no puedan ser interceptados.

**Para mejorar la seguridad pasiva:**

- La realización de copias de seguridad de los datos en más de un dispositivo o en distintas ubicaciones físicas.
- Realizar planes de escanear y limpiar los equipos dentro y fuera de las instalaciones para controlar y evitar ataques de malware.

- Mantener las versiones del antivirus actualizadas y realizar pruebas de vulnerabilidad de acuerdo a recomendaciones del proveedor.

**Con respecto a la intranet:**

-La Intranet de la empresa posee clave de acceso al servidor VPN el cual cuenta con antivirus. Se recomienda la creación de credenciales de acceso con contraseñas seguras para cada empleado las cuales a la vez sirvan para delimitar el acceso a los directorios de la intranet. También se recomienda instalar un firewall.

**Con respecto a la seguridad física:**

-Debido a que la mayoría del personal se encuentra trabajando de forma remota, no se ve necesario hacer una gran inversión en dispositivos físicos de protección, se recomienda invertir recursos en sistemas de redundancia y respaldo de datos para garantizar que la información confidencial de la empresa no siempre esté disponible y respaldada en caso de cualquier ataque, robo o pérdida de información.

**Medidas de seguridad sugeridas para el uso de los empleados:**

- El personal de la empresa debe mantenerse en constante capacitación haciendo énfasis en los errores registrados.

**Paso 6:** Se recomienda seguir el plan rigurosamente y periódicamente revisarlo y actualizarlo, respetando los pasos para lograr el objetivo de la eficiencia, normativa y gestión de recursos.