**CONSIGNA**

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. 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.

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.

**Seguridad Lógica**:

* Roles para restricción de acceso a los distintos perfiles.
* Cifrado de datos para mails / mensajes, password de acceso.
* Implementación de un correcto Antivirus y firewalls

**Seguridad Física**: Consiste en el establecimiento de técnicas que permiten resguardar de cualquier tipo de daños a los equipos en los cuales se almacena los activos de una organización —sus datos

* UPS.
* Respaldo de datos
* Sistema de información redundante

**Seguridad Activa**:

* Uso y empleo adecuado de contraseñas, (combinación entre letras, números, mayúsculas y otros caracteres).
* Uso de software de seguridad informática, (antivirus, anti espías y cortafuegos).
* Encriptar los datos importantes.

**Seguridad Pasiva**:

**Realizar copias de seguridad de los datos en más de un dispositivo como implementación de mejorar en seguridad Pasiva. y/o en distintas ubicaciones físicas.**

**Controles de medida de seguridad y / o prevención**

Como primer medida debemos auditar a través de acciones que nos ayuden a detectar vulnerabilidades, ya sea dentro del sistema de redo también sobre algún equipo informático. Para ello sugerimos los siguientes pasos:

* Verificar la red (construcción y arquitectura, definición de roles para manipular información )
* Restringir el acceso a la red mediante los roles definidos en el paso anterior. Clasificación de los mismos según el tipo de información: puede ser **sensible y esencial**.
* Auditar el estado de la seguridad informática a nivel general, concientizar a usuarios con medidas de seguridad.

**Medidas proactivas**

-**directivas**: proponemos el bloqueo de la actividad en algunas páginas de internet, las cuales son consideradas nocivas para la seguridad de la red de la compañía.

- **preventiva**: capacitar en materia de pishing, smithing, vishing, malware, spyware.

- **disuasiva**: si un usuario está utilizando info de la red y un segundo usuario quiere ingresar al mismo recurso se genera una notificación para ambos.

**Medidas reactivas**

-**detectivas**: implementar un sistema de soft que avise al usuario ante posibles ataques que garantice la seguridad del sistema y los equipos informáticos de la empresa.

-**correctivas**: ante la detección de una amenaza nuestro sistema de software desvincula el acceso remoto a Intranet, en busca de resguardar la integridad de la seguridad / información.

**INTEGRANTES**: Molina David-Tomas Coronel-Alejo Jorja-Julian Maccor