**Actividad 5:**

Sobre una instalación de sistemas informáticos en red, por ejemplo, la del aula, describe qué medidas de seguridad física y ambiental están tomadas y qué otras se podrían tomar para mejorar la seguridad.

El aula dispone de varias medidas de seguridad físicas, una de ellas es la video vigilancia ya que dispone de varias cámaras que permiten controlar el acceso físico de los alumnos y otras personas a las aulas. Además, hay una persona en recepción controlando la entrada y salida para que ninguna persona sin acceso pueda acceder a las aulas o salir de ellas con material que no esté permitido llevarse.

Una medida de seguridad que se podría implementar para mejorar la seguridad sería la implementación de un generador eléctrico que pueda mantener el sistema informático operativo en caso de fallo en el suministro eléctrico.

**Actividad 6:**

Repite el ejercicio anterior sustituyendo los elementos de seguridad física por elementos de seguridad lógica.

Los ordenadores tienen diferentes cuentas de usuario con contraseña para cada uno de los alumnos. Además, cada usuario tiene su propio rol dentro del sistema lo que le proporciona servicios concretos.

Una medida que se podría implementar sería un nuevo SO que pudiera estar actualiza constantemente ya que Windows 7 no dispone de más soporte por parte de Microsoft. Además, se podrían instalar en los ordenadores algunas aplicaciones tipo antivirus o antimalware.

**Actividad 7:**

A partir de la información proporcionada con los niveles de seguridad, elabora un mapa conceptual de las características básicas necesarias para la clasificación de un sistema dentro de los niveles estandarizados de seguridad TCSEC.

Procesos de seguridad mediante métodos matemáticos

Registra los intentos de acceso. Varios niveles de autorización

Auditoría exhaustive sobre la seguridad

Gestiona la herencia de permisos

Seguridad multinivel entre distintas capas

Requiere la autenticación. Existe un superusuario

Sin protección

Nivel A1

Nivel B3

Nivel B2

Nivel B1

Nivel C1

Nivel D

Nivel C2

Define la siguiente jerarquía de niveles

Estándar TCSEC

**Actividad 8:**

¿Cuáles son las cuatro fases de un análisis de investigación forense? ¿Podrías poner ejemplos de actividades específicos de cada una de las fases?

Las cuatro fases de un análisis forense son:

1. Identificación y evaluación de incidentes

* Localizar los dispositivos afectados e intentar identificarlos dentro del sistema (versión del HW y del SW, aplicaciones instaladas, ubicación en la empresa, etc…)
* Comprobar en el registro la identidad de la persona que utiliza el sistema, así como la del administrador que lo gestiona (nombre y apellidos, horario de entrada y salida, rol en la empresa, etc…)

1. Preservación de la incidencia o adquisición de los datos

* Realizar la clonación a bajo nivel (bit a bit) de los discos duros en los sistemas afectados.
* A la hora de manejar el material afectado y, en especial, los discos es muy importante seguir con las medidas de seguridad especificadas en el plan de contingencia para que se pueda recoger la evidencia de la forma más clara posible, esto incluye el uso de guantes y bolsas herméticas, entre otras medidas con el fin de manipular el material de forma segura

1. Análisis de la evidencia

* Comprobar el registro del Sistema Operativo, del cortafuegos o cualquier otro elemento que realice una monitorización.
* Además, se puede realizar un análisis físico de los sistemas, si se tiene sospechas ante un posible intruso

1. Documentación y reporte del incidente.

* Elaborar un informe pericial con toda la información obtenida durante la investigación, presentando de manera objetiva los datos obtenidos y los procedimientos realizados.
* Una vez elaborado, se deberá reportar dicho informe a las autoridades oportunas y en caso de ser necesario, presentar las medidas legales oportunas

**Actividad 9:**

Trabajas en una auditoría de seguridad informática. Llega un nuevo cliente que desea conocer la situación de su empresa y si es aceptable o podría mejorar. Durante la entrevista tomas las siguientes notas:

* El edificio tiene un servicio de vigilancia a través de una empresa externa. Por reducción del presupuesto, ahora solo hay un vigilante que también atiende el edificio del otro lado de la calle.
* El CPD tiene otro vigilante, de otra compañía, que también atiende el teléfono de la centralita a partir de las tres, cuando termina el turno del recepcionista.
* Existe una falta clara de personal de seguridad en la empresa, para mayor seguridad sería muy recomendable que los vigilantes fueran de la misma empresa o incluso la propia empresa debería considerar contratar un total de tres vigilantes para que garanticen el control de acceso físico de manera eficaz en cada uno de los edificios. Si es necesario también se debería contratar otro recepcionista, pero un vigilante nunca debería ausentarse de su puesto de trabajo para realizar dichas funciones.
* Para entrar al CPD, cada informático tiene una tarjeta particular, si bien hay una en el cajón de la mesa del vigilante para el personal de limpieza o por si ocurre una emergencia.
* Tener una tarjeta al alcance de cualquiera es una gran vulnerabilidad que puede poner en riesgo el CPD. Se debería dar una tarjeta única e intransferible a cada trabajador que necesite entrar al CPD. En caso de necesidad se deberá consultar con el administrador que será el único que pueda otorgar acceso a dicho edificio.
* Una vez a la semana se hace la copia de seguridad. Como solo disponen de un dispositivo de cinta, los cuatro servidores se reparten cada semana del mes. Dado que solo hay un vigilante para el CPD, las cintas se dejan dentro de la sala, cada una encima de su servidor (cada servidor tiene una cinta en exclusiva).
* Las copias de seguridad se deberían hacer de manera rutinaria en un día y una hora concreta. Además, estás no se deberían guardar nunca en la misma sala que los servidores, sería recomendable que se custodiaran en otra sala o incluso en uno de los otros edificios.
* El edificio pertenece al patrimonio histórico y no admite reformas en la fachada. Por tanto, no ha sido posible instalar equipos de aire acondicionado en el CPD. Para combatir el calor que desprenden los ordenadores, las ventanas están siempre abiertas.
* Tener siempre las ventanas abiertas conlleva un alto riesgo que puede causar mucho daño al sistema informático en caso de lluvia o una humedad elevada. Una solución sería instalar un sistema de refrigeración que no modifique la fachada del edificio o invertir en una muy buena refrigeración para los servidores.
* Cada servidor tiene un disco duro de alta gama, que no ha fallado nunca.
* Pese a que los discos duros sean fiables, todo servidor debe instalarse con un sistema RAID (en espejo por lo menos) para que la rotura en un disco no deja al sistema inutilizable.
* Los servidores tienen doble fuente de alimentación, por si se estropea alguna.
* Aparte de la doble fuente de alimentación sería recomendable disponer de un sistema de alimentación interrumpida que pueda proveer a los servidores de electricidad durante un periodo razonable de tiempo en caso de fallo en el suministro eléctrico.
* El presidente y el contable tienen cada uno un portátil de la empresa. El disco duro de estas máquinas no está cifrado porque no se arriesgan al desastre que supondría olvidar la contraseña.
* Toda la información que se maneja en la empresa tiene que estar siempre cifrada, de no ser así se corre un gran riesgo en caso de robo o escucha de la información. Es posible implementar un sistema de recuperación de contraseñas seguro en este caso.
* Los ordenadores tienen dos usuarios: uno para las tareas normales y otro para cuando necesitan realizar alguna instalación o modificar un parámetro del sistema operativo. Los empleados saben cuándo deben usar cada uno.
* Los usuarios “normales” no deberían poder ni instalar, ni desinstalar, ni modificar los programas o archivos que están en el ordenador, sólo el administrador debería ser capaz de realizar dichas funciones. En caso de necesidad, un usuario deberá acudir al administrar para realizar alguna de estas modificaciones

Termináis por hoy la entrevista porque ha sido una reunión muy larga. Todavía no has redactado el informe final, pero ¿encuentras algo que mejorar? ¿Qué alternativa le puedes proponer?