Número i nom del curs	[IFCT0109_CEN] Seguretat dels sistemes d'informació
Mòdul Formatiu que s'avalua	MF0486_3 Seguretat en equips informàtics

Nom i Cognoms de l'alumne/a	Diego Fernando Mucci
NIF de l'alumne/a	X1766856L
Data de la prova	20/04/2024
Signatura	Diego Fernando Mucci

INSTRUCCIONS DE LA PROVA

- En aquest full trobarà la informació necessària per a la realització de la prova.
- Abans de resoldre la pràctica llegeixi amb atenció l'enunciat de l'exercici i comprovi que té tots els materials i equipament necessari.
- Per qualsevol aclariment consulti a l'avaluador/ i/o formador/a.
- Cas de ser necessari, utilitzi els equips de protecció individual necessaris per la realització de la pràctica tenint en compte les normes de seguretat i higiene.

DESCRIPCIÓ DE LA PRÀCTICA	
DENOMINACIÓ	Análisis de riesgos, protección de datos de carácter personal y seguridad de la información.
ESPECIFICACIONS TÈCNIQUES	Lee el enunciado del ejercicio y responde a las preguntas. Puedes consultar cualquier fuente para su realización. Dispones de 4 horas para presentar la prueba práctica, que entregarás en un documento pdf con tus soluciones justificadas.
MATERIAL	Tu propio ordenador
TEMPS	Cuatro horas

SUPUESTO

La empresa IRON S.L. proporciona un servicio diario de resúmenes de prensa personalizados, recopilando noticias relevantes para cada cliente.

Utiliza un software alojado en un servidor en su sede, ubicada en una zona rural de España. Este programa opera durante la noche, buscando en medios digitales y almacenando en una base de datos (BBDD) las URLs pertinentes junto con los datos de contacto de los clientes.

Cada día, a las 6 a.m., el sistema genera y envía un correo electrónico a los clientes con las URLs recopiladas. Aunque la conexión a internet se realiza mediante ADSL de cobre, debido a la falta de infraestructura de fibra óptica en la región, es lo suficientemente rápida para el envío de correos.

Adicionalmente, cuentan con un router 4G como respaldo, garantizando así una conexión estable, que no ha presentado interrupciones en los últimos tres años.

Sin embargo, los cortes de electricidad son comunes en la localidad durante la temporada de lluvias.

El servidor, que también se usa para tareas generales como navegación web, gestión de ofertas y contabilidad, e incluso para la descarga ocasional de películas, no es un equipo dedicado exclusivamente al servicio de resúmenes de prensa.

Activitat 1 (2 punts)	Identifica activos, descríbelos y calcula de forma cualitativa el valor de los mismos en cuanto a disponibilidad. Utiliza la clasificación Magerit para la catalogación de activos.
Activitat 2 (2 punts)	Identifica y describe las amenazas. Utiliza Magerit para su clasificación y determina las dimensiones susceptibles de verse afectades y los grupos de activos que pudieran verse afectados
Activitat 3 (2 punts)	Determina el riesgo de que se materialicen las amenazas, calculando de manera cualitativa el impacto sobre los activos y la frecuencia con la que se pueden materializar las amenazas. Crea las tablas de impacto, frecuencia y riesgo.
Activitat 4 (2 punts)	Propón contramedidas para mejorar la situación de riesgo resultante y explica que harías tras implementar las contramedidas propuestas.
Activitat 5 (2 punts)	¿Garantiza IRON S.L. el cumplimiento de la ley de protección de datos personales al almacenar y procesar datos de contacto de los clientes en su base de datos? Si no lo garantiza, explica el motivo y en su caso cómo podría garantizarlo. Propón al menos tres medidas para que se garantice la normativa en caso de ser necesario

PUNTUACIÓ FINAL PROVA PRÀCTICA					
ACT 1	**ACT 2**	**ACT 3**	**ACT 4**	**ACT 5**	***PUNTUACIÓ FINAL***

OBSERVACIONS

Signatura formador/a	Signatura responsable acció formativa

Actividad 1

Identifica activos, descríbelos y calcula de forma cualitativa el valor de los mismos en cuanto a disponibilidad. Utiliza la clasificación Magerit para la catalogación de activos.

Los activos que tenemos dentro de la empresa son los siguientes:

ACTIVOS
Resúmenes de prensa personalizados
Software
Instalaciones (España)
Bases de datos (BBDD)
URLs noticias
Datos contacto clientes
Correo electrónico
ADSL
Router 4G
Electricidad
Servidor
Personal
Navegador web

Lo siguiente que debemos hacer es catalogar los activos de la tabla anterior según la clasificación Magerit, para ello nos iremos al *Libro de catálogo de elementos* de Magerit.

ACTIVOS	CLASIFICACIÓN MAGERIT
Resúmenes de prensa personalizados, Correo electrónico	[S] Servicios
Software, Navegador web	[SW] Aplicaciones (software)
Instalaciones (España)	[L] Instalaciones
Bases de datos (BBDD), URLs noticias, Datos contacto clientes	[D] Datos / Información
Personal	[P] Personal
ADSL	[COM] Redes de comunicaciones
Router 4G, Servidor	[HW] Equipos informáticos (hardware)
Electricidad	[AUX] Equipamiento auxiliar

Seguidamente vamos a calcular de forma cualitativa el valor de estos activos en cuanto a la dimensión de disponibilidad. Este valor se lo daremos nosotros según nuestro criterio.

Dimensión Disponibilidad	Descripción
Muy alto	El activo es esencial para el funcionamiento de la organización y su no disponibilidad supone trastornos muy graves para la actividad de la empresa.
Alto	El activo es importante para el funcionamiento de la empresa y su no disponibilidad supone trastornos graves para la actividad de la empresa.
Medio	El activo es relevante para el funcionamiento de la empresa y su no disponibilidad supone trastornos moderados para la actividad de la empresa.
Bajo	El activo es poco relevante para el funcionamiento de la empresa y su no disponibilidad supone trastornos leves para la actividad de la empresa.

ACTIVOS	CLASIFICACIÓN MAGERIT	DISPONIBILIDAD
Resúmenes de prensa personalizados, Correo electrónico	[S] Servicios	Muy alto
Software, Navegador web	[SW] Aplicaciones (software)	Alto
Instalaciones (España)	[L] Instalaciones	Medio
Bases de datos (BBDD), URLs noticias, Datos contacto clientes	[D] Datos / Información	Muy alto
Personal	[P] Personal	Bajo
ADSL	[COM] Redes de comunicaciones	Medio
Router 4G, Servidor	[HW] Equipos informáticos (hardware)	Alto
Electricidad	[AUX] Equipamiento auxiliar	Alto

A los servicios le asignamos un valor “Muy alto”, ya que es el núcleo y sustento principal de la empresa.

A las aplicaciones software, a pesar de que son esenciales para la generación del servicio diario de resúmenes de prensa, le asignamos un valor “Alto”, ya que en el caso de que falle o sea atacado, la empresa podría disponer de otro de sustitución.

A la localización física de la empresa, es decir a las instalaciones, que están en España, le damos un valor “Medio”, ya que podría ser fácilmente reubicada en otro lugar donde existieran menos cortes de electricidad.

A los datos que se almacenan en las bases de datos le damos un valor “Muy alto” ya que aquí se almacenan los datos de contacto de los clientes, los cuales se han de proteger y han de estar siempre disponibles para hacerles llegar sus resúmenes diarios de prensa.

Al personal le asignaríamos el valor “Bajo” porque en el caso de no poder contar más con algún empleado se podría contratar a otro/s.

A las redes de comunicaciones le damos un valor “Medio”, ya que es esencial para ofrecer el servicio de la empresa, pero en el caso de que falle la comunicación vía ADSL, la empresa dispone de un router 4G para garantizar así una conexión estable.

A los equipos informáticos o hardwares le damos un valor “Alto”, ya que son indispensables para el desarrollo del servicio que proporciona la empresa, pero podría disponer de otros hardware de sustitución.

A la electricidad, le asignamos un valor “Alto” dado que también es esencial para hacer funcionar los equipos y las redes de comunicación. Pero debido a que los cortes son frecuentes en temporada de lluvias, la empresa seguramente cuente con uno o varios generadores para poder mantener el servicio en estas ocasiones.

Actividad 2

Identifica y describe las amenazas. Utiliza Magerit para su clasificación y determina las dimensiones susceptibles de verse afectades y los grupos de activos que pudieran verse afectados.

Las amenazas presentes en la empresa serian:

- Cortes de electricidad. Son frecuentes en temporada de lluvias.
- Daños por agua durante la temporada de lluvias.
- Malware. El enunciado nos dice que el servidor no es un equipo dedicado exclusivamente al servicio de resúmenes de prensa, sino que se realizan ciertas actividades como la descarga ocasional de películas, lo cual podría generar la intrusión de software dañinos.
- Averías de hardware. Debido a ese uso que se le da a los equipos, fuera de las necesidades de la empresa, también se podrían ocasionar averías de hardware.

Amenazas	Clasificación Magerit	Activos afectados	Dimensiones afectadas
Cortes de electricidad	[I.6] Corte del suministro eléctrico	HW, Media, AUX	Disponibilidad
~~Daños por agua~~	~~[N.2] Daños por agua~~	~~HW, Media, AUX Instalaciones (L)~~	~~Disponibilidad~~
Malware	[A.8] Difusión de software dañino	SW	Disponibilidad, Integridad y Confidencialidad
Averías de Hardware	[I.5] Avería de origen físico o lógico	HW, Media, AUX, SW	Disponibilidad

Actividad 3

Determina el riesgo de que se materialicen las amenazas, calculando de manera cualitativa el impacto sobre los activos y la frecuencia con la que se pueden materializar las amenazas. Crea las tablas de impacto, frecuencia y riesgo.

- Primero creamos una tabla de valoración del impacto que tendrían las amenazas en cuanto a la dimensión de la disponibilidad del activo. Para ello vamos a establecer primero en una tabla los valores cualitativos que le daremos a las amenazas.

Impacto para la Disponibilidad	
Descripción	**Cualitativo**
La amenaza provoca la interrupción total y prolongada del servicio o el activo, lo que tiene un impacto catastrófico en la disponibilidad.	Muy alto
La amenaza tiene interrupciones significativas y prolongadas en el servicio o el activo, lo que resulta en una pérdida sustancial de disponibilidad.	Alto
La amenaza causa interrupciones ocasionales o limitadas en el servicio o el activo, lo que afecta moderadamente a la disponibilidad.	Medio
La amenaza tiene un impacto mínimo en la disponibilidad del servicio o el activo, con interrupciones breves y fácilmente gestionables.	Bajo

Impacto para la Disponibilidad	
Amenaza	**Valoración**
Corte de suministro eléctrico	Medio
Daños por agua	Alto
Difusión de software dañino	Muy alto
Averías de hardware	Alto

El impacto que tendría un corte de suministro eléctrico en cuanto a la disponibilidad de los activos sería “Medio”. Como estos cortes son comunes en la temporada de lluvias, la empresa ya está preparada para esta amenaza y cuenta con uno o varios generadores para disponer de electricidad cuando ocurran estas situaciones.

Si se ocasionaran daños por agua, esto tendría un impacto “Alto”, ya que si se dañan los equipos, el servicio de la empresa podría verse afectado durante la noche que es cuando opera el software alojado

en el servidor de la sede de la empresa. No se le asigna un valor “Muy alto” porque la empresa cuenta con cierta protección dado que son comunes las temporadas de lluvias.

En el caso de que la empresa sea atacada por un software dañino debido a la descarga de contenido que no es imprescindible para el funcionamiento de la empresa, esto podría tener un impacto “Muy alto” ya que podría provocar la interrupción total y prolongada del servicio o activo al cual afecta. Además, no solo afectaría a la disponibilidad del software necesario para la actividad de la empresa, sino que también podría afectar a la confidencialidad e integridad de la información y datos de la empresa y clientes.

Si se dieran averías de hardware, esto tendría un impacto “Alto” ya que podría existir una interrupción prolongada hasta la reanudación del servicio.

- Seguidamente creamos una tabla de valoración de la frecuencia con la que se pueden producir las amenazas. Estableceremos también, lo que significaría una frecuencia muy alta, alta, media o baja de ocurrencia.

Frecuencia	
Descripción	**Cualitativo**
Tres o más veces al año	Muy alto
Una o dos veces al año	Alto
Una vez cada dos a cuatro años	Medio
Una vez cada cinco años o más	Bajo

Frecuencia	
Amenaza	**Cuantitativo**
Corte de suministro eléctrico	Alto
Daños por agua	Bajo
Difusión de software dañino	Muy alto
Averías de hardware	Medio

- Creamos la tabla de riesgo, la cual se obtiene multiplicando el valor de la frecuencia por el valor del impacto. Esta tabla nos va a servir para saber posteriormente el riesgo de cada una de las amenazas.

Tabla de riesgo				
Frecuencia/Impacto	Muy alto (4)	Alto (3)	Medio (2)	Bajo (1)
Muy alto (4)	Muy alto (16)	Alto (12)	Medio (8)	Bajo (4)
Alto (3)	Alto (12)	Alto (9)	Medio (6)	Bajo (3)
Medio (2)	Medio (8)	Medio (6)	Bajo (4)	Bajo (2)
Bajo (1)	Medio (4)	Bajo (3)	Bajo (2)	Bajo (1)

Siendo
- 1-4: Bajo
- 5-8: Medio
- 9-12: Alto
- 13-16: Muy alto

A partir de la tabla de la actividad 2, en la cual vemos a que activos afecta cada amenaza, elaboraremos otra tabla para saber el riesgo de estas tres amenazas sobre los activos. También nos ayudaremos de la tabla anterior para saber el riesgo de cada amenaza sobre cada activo. Recordando que:

Riesgo = Impacto * Frecuencia

		Amenazas			
Activos	**Clasificación Magerit**	**Corte suministro eléctrico**	**Daños por agua**	**Software dañino**	**Averías de Hardware**
Resúmenes de prensa personalizados, Correo electrónico	[S] Servicios				
Software, Navegador web	[SW] Aplicaciones (software)			Muy alto	Medio
Instalaciones (España)	[L] Instalaciones		Bajo		
Bases de datos (BBDD), URLs noticias, Datos contacto clientes	[D] Datos / Información				
Personal	[P] Personal				
ADSL	[COM] Redes de comunicaciones				
Router 4G, Servidor	[HW] Equipamiento informático (hardware)	Medio	Bajo		Medio
Electricidad	[AUX] Equipamiento auxiliar	Medio	Bajo		Medio

Actividad 4

Propón contramedidas para mejorar la situación de riesgo resultante y explica que harías tras implementar las contramedidas propuestas.

Tal y como hemos comprobado, nuestro mayor riesgo es el software dañino o malware. Por lo tanto, lo primero que tendremos que tratar de lograr es: eliminar el riesgo aplicando las salvaguardas correspondientes y en el caso de que eso no sea posible, vamos a minimizar ese riesgo o transferirlo.

Tres contramedidas o salvaguardas posibles para eliminar, minimizar, reducir o transferir la amenaza de malware en la empresa podrían ser:

- Implementar políticas de acceso y privilegio para limitar el acceso de los usuarios solo a los recursos y datos necesarios para realizar sus funciones.
- Implementar softwares de seguridad como antivirus o firewalls, para detectar y prevenir la ejecución de software malicioso.
- Concientizar y capacitar al personal para evitar la descarga de contenido indebido.

Tras implementar estas salvaguardas, se debería volver a realizar el análisis de riesgos. Veríamos como disminuiría la frecuencia de ocurrencia de software dañino y por lo tanto su riesgo se vería disminuido. Pero cuando se implementan salvaguardas o contramedidas, es posible que aparezcan nuevas amenazas. Por último, una vez hecho nuevamente el nuevo análisis de riesgo con las salvaguardas aplicadas, se debería evaluar el riesgo residual.

Actividad 5

¿Garantiza IRON S.L. el cumplimiento de la ley de protección de datos personales al almacenar y procesar datos de contacto de los clientes en su base de datos?
Si no lo garantiza, explica el motivo y en su caso cómo podría garantizarlo. Propón al menos tres medidas para que se garantice la normativa en caso de ser necesario.

Con la información proporcionada en el enunciado, no se especifica ninguna medida que aplique la empresa para garantizar el cumplimiento de la ley de protección de datos personales al almacenar y procesar datos de contacto de los clientes en su base de datos. Por lo tanto, y debido a que el servidor donde se aloja la base de datos es usado para otros fines que no van relacionados con la actividad de la empresa, podemos suponer que no garantiza el cumplimiento de dicha ley.

Tres medidas posibles para poder garantizar el cumplimiento de la ley de protección de datos personales podrían ser:

- **Implementación de medidas de seguridad adecuadas**: IRON S.L. debe asegurarse de que la base de datos que contiene los datos de contacto de los clientes esté protegida con medidas de seguridad adecuadas, como cifrado de datos, acceso restringido y controles de acceso.
- **Obtención de consentimiento informado:** Antes de almacenar y procesar los datos de contacto de los clientes, IRON S.L. debería obtener su consentimiento explícito e informado. Esto implica explicar claramente cómo se utilizarán los datos y obtener el consentimiento activo de los clientes.
- **Formación en protección de datos:** La empresa debería proporcionar formación en protección de datos a su personal para asegurarse de que comprenden sus responsabilidades y cómo manejar adecuadamente los datos personales de los clientes

Plan de recuperación y backup, ...

9.5/10, muy buen trabajo