UNIDAD 1: INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

ACTIVIDADES -PÁG. 11

1. **La biblioteca pública de una ciudad tiene mobiliario, libros, revistas, microfilms, varios ordenadores para los usuarios en donde pueden consultar libros electrónicos, y un ordenador en el que la bibliotecaria consulta títulos, códigos, referencias y ubicación del material bibliográfico.**

   Indica a continuación de cada elemento con un SÍ, si forma parte del sistema informático de la biblioteca y con un NO si no forma parte de él:
   a) Libros y revistas colocados en las estanterías. NO
   b) Mobiliario. NO
   c) Microfilms. NO
   d) **Libros electrónicos. SÍ** puesto que son información en formato digital.
   e) Ordenadores de los usuarios. SÍ
   f) Ordenador de la bibliotecaria. SÍ
   g) Datos almacenados en el ordenador de la bibliotecaria. SÍ
   h) Bibliotecaria. NO

2. **De los elementos relacionados en la pregunta anterior, ¿cuáles pertenecen al sistema de información de la biblioteca?**

   Todos

3. **Un incendio fortuito destruye completamente todos los recursos de la biblioteca. ¿En qué grado crees que se verían comprometidas la integridad, la confidencialidad y la disponibilidad de la información?**

   La integridad se vería comprometida totalmente, puesto que desapareció toda la información. Lo mismo ocurre con la disponibilidad. En cuanto a la confidencialidad, con los datos de que disponemos, no tendría por qué verse comprometida.

4. **El informático que trabaja para la biblioteca, ¿forma parte del sistema informático de la misma?**

   No.

5. **El ordenador de la biblioteca tiene un antivirus instalado, ¿esto lo hace invulnerable?**

   No, en absoluto. Puede sufrir cualquier otro daño, por ejemplo físico: ser robado o destruido. El antivirus tampoco vuelve invulnerable al equipo si no está actualizado.

6. **¿A qué se deben la mayoría de los fallos de seguridad? Razona tu respuesta.**

   A la acción de las personas, unas veces por errores humanos, por falta de capacitación profesional o por mala fe, tanto en lo que respecta a la seguridad física como a la seguridad lógica. Y esto ocurre porque prácticamente todo el sistema de información está en manos del personal de la organización y de otras personas externas que interactúan con él.

7. **¿Podrías leer un mensaje encriptado que no va dirigido a ti? Busca en internet algunos programas que encriptan mensajes.**

   Depende del nivel de seguridad de la encriptación. En principio cualquier persona puede leer un mensaje cifrado o encriptado si posee la clave de lectura, pero los programas de encriptación tienen agregadas otras funciones que aseguran en un alto porcentaje que el mensaje no podrá ser leído por nadie que no sea el destinatario.

8. **¿La copia de seguridad es una medida de seguridad pasiva?**

   Tener hechas copias de seguridad es una medida de seguridad pasiva puesto que se utilizarán cuando un ataque destruya la información aunque sea en parte.

9. **¿Qué propiedades debe cumplir un sistema seguro?**

   El que garantiza la confidencialidad, disponibilidad e integridad de la información.

10. **¿Qué garantiza la integridad?**

    Que los datos no han sido alterados ni destruidos de modo no autorizado.

ACTIVIDADES-PÁG. 15

11. **La ventana de un centro de cálculo en donde se encuentran la mayor parte de los ordenadores y el servidor de una organización se quedó mal cerrada. Durante una noche de tormenta, la ventana abierta ¿constituye un riesgo, una amenaza o una vulnerabilidad? Razona la respuesta.**

    La ventana abierta es una vulnerabilidad del sistema.

12. **Teniendo en cuenta las propiedades de integridad, disponibilidad y confidencialidad, indica cuáles de estas propiedades se verían afectadas por:**

    a) **Una amenaza de interrupción.** Disponibilidad
    b) **Una amenaza de interceptación.** Confidencialidad
    c) **Una amenaza de modificación.** Integridad
    d) **Una amenaza de fabricación.** Integridad

13. **Pon un ejemplo de cómo un sistema de información podría ser seriamente dañado por la presencia de un factor que se considera de poca relevancia y que explique de alguna manera que «La cadena siempre se rompe por el eslabón más débil».**

    Ejemplo 1: Los usuarios de los ordenadores de una oficina son buenos profesionales, conocen y practican la política de seguridad de la empresa y son profesionales responsables, pero el personal que se ocupa de la limpieza y que pertenece a la misma empresa es algo irresponsable y olvida alguna vez cerrar las puertas con llave o las ventanas. El personal de limpieza es el eslabón más débil de la cadena y hace vulnerable al sistema.

    Ejemplo 2: La planta de un edificio alberga el sistema informático de una empresa. Esa planta está dotada de todas las medidas físicas de seguridad en cuanto a cierres, acceso de personal con contraseñas, extintores, etc., pero hace tiempo que no actualizan los antivirus e incluso hay equipos sin antivirus instalado. Tanto si esos equipos son independientes como si están en red con los demás, la falta de antivirus o de actualizaciones es una vulnerabilidad del sistema. La seguridad antivirus es en este caso el eslabón débil de la cadena.

14. **¿Qué elementos se estudian para hacer un análisis de riesgos?**

    Activos, amenazas, riesgos, vulnerabilidades, ataques, impactos.

ACTIVIDADES-PÁG. 18

15. Investiga el término *war driving*, que también puede expresarse como *wardriving* o *war xing*. ¿Crees que el *war driving* constituye un riesgo contra la confidencialidad?

El objetivo del *war driving* es encontrar redes inalámbricas abiertas para utilizarlas. En una red abierta puede interceptarse información, por lo que existe un riesgo contra la confidencialidad.

16. ¿Qué relación hay entre servicios de seguridad y mecanismos de seguridad?

Los mecanismos de seguridad dan determinados servicios: los servicios de seguridad.

17. ¿Qué es el SSID de una red WiFi?

Es el nombre que damos a nuestra red inalámbrica (o el que trae por defecto).

18. ¿Podrías explicar qué significa encriptar un mensaje? Inventa un sencillo sistema de encriptación (codificación). Imagina que envías a otra persona unas palabras codificadas según tu sistema inventado. ¿Qué necesita tener o saber la persona que recibe tu mensaje para poder descifrarlo?

Encriptar es un anglicismo y no lo recoge nuestro diccionario de la Lengua Española. Es sinónimo de cifrar o codificar. Por lo tanto encriptar un mensaje es traducirlo a otro código. Un sistema muy simple de encriptación podría ser dar a cada letra del abecedario el valor de un número consecutivo:
A=1, B=2, C=3…
Para traducir, por ejemplo, la palabra HADA al nuevo código, lo escribiríamos 8141.

19. De los siguientes dispositivos indica cuáles son preventivos, detectores o correctores:

a) Cortafuegos *(firewal).* Corrector: cuando ocurre un incendio se minimizan sus efectos si un cortafuegos impide que el fuego pase a otras zonas.
b) Antivirus. Previene la entrada de virus, los detecta si se han introducido en el disco u otro dispositivo y los elimina, por lo tanto tiene las tres dimensiones: preventiva, detectora y correctora.
c) Extintor de fuegos. Corrector, porque extingue el fuego (o lo atenúa mientras llegan los bomberos) y así reduce el impacto.
d) Detector de humos. Detector.
e) Firma digital. Preventiva, porque impide la entrada de una persona no autorizada a un determinado recurso o documento.

ACTIVIDADES-PÁG. 19

20. Imagina esta situación: Quieres presentar a tu jefe una brillante idea que puede interesar a la competencia, pero te encuentras de fin de semana en un pueblecito donde los teléfonos móviles no funcionan, por suerte te has llevado tu portátil y el hotel rural donde te encuentras alojado dispone de servicio de internet. Así que decides enviarle un correo electrónico pero sin encriptar. Explica los peligros de este procedimiento.

Se supone que el hotel dispone de una red wifi abierta, lo cual ya constituye un riesgo de interceptación. En cualquier caso los mensajes de correo de gran trascendencia tendrían que encriptarse porque con las técnicas de ingeniería social puede interceptarse la información entre el origen y el destino.

21. Investiga qué es la esteganografía.

Una técnica que consiste en esconder un mensaje dentro de cualquier soporte u objeto, de modo que ni siquiera existe constancia de que el mensaje existe.

Un ejemplo es el que se describe en Las Historias de Herodoto: a un mensajero se le rapa la cabeza, se le tatúa un mensaje en el cuero cabelludo y luego se le deja crecer el cabello. Cuando se le envía al destinatario, este deberá raparle de nuevo la cabeza y descubrirá el mensaje.

22. ¿Cómo escogerías una clave segura de acceso al ordenador de una empresa donde se guardan datos confidenciales de clientes?

Dada la importancia de la información, ya que se trata de datos confidenciales de personas, nunca se utilizarán como contraseña palabras comunes como nombres de personas, números de teléfono, de documentos de identidad, fechas o palabras que existen en el diccionario y que encontrarían fácilmente los programas rastreadores de claves. En principio una buena clave será larga, contendrá caracteres que no estén en el abecedario (como %, &, #, espacios…) y mezclará mayúsculas, minúsculas y números.

23. Trabajas como técnico de informática y te llega una llamada de una oficina. Un empleado hacía cada semana una copia de seguridad de la carpeta Documentos Importantes. La copia la guardaba en otra partición del mismo disco duro. Una tormenta eléctrica ha dañado el disco y un experto en informática no ha hallado modo de restablecer su funcionamiento. Te piden que te acerques a la oficina para ver si existe la posibilidad de recuperar al menos los datos.

a) **¿Podrás recuperar los datos originales?** Si ya se ha verificado por un experto informático que el disco es irrecuperable, difícilmente podrá hacerse, aunque existen programas informáticos que consiguen recuperar al menos parte de la información de discos muy dañados, aunque el resultado no siempre está exento de errores de integridad.
b) **En su defecto, ¿podrán recuperarse los que hay en la copia de seguridad?** Existe el mismo problema que en los datos originales, puesto que los dos se encuentran en el mismo soporte dañado.
c) **A tu juicio, ¿el empleado ha cometido alguna imprudencia con la copia de seguridad?** Sí. Si la información es muy importante no debería haberla guardado en el mismo disco duro, pues una avería del mismo o su robo le haría perder tanto los originales como las copias de seguridad.

ACTIVIDADES-PÁG. 22

24. Investiga qué es un test de intrusión.

Un sistema para valorar la vulnerabilidad de la red informática de una organización, así como la de todos los dispositivos a los que se puede acceder desde internet, como routers, firewalls, servidores web, de correo, de noticias, etc. El test analiza todos los puntos que podrían ser vulnerables a ataques de intrusos informáticos utilizando sus mismas técnicas.

25. Tu jefe te dice que ha detectado que el rendimiento de los trabajadores ha bajado considerablemente desde que la empresa tiene acceso a internet. Te pide que le propongas una solución.

La creación de una política de seguridad en la empresa. Si ya existe la política de seguridad, la formación de los empleados para cumplirla. Además se pueden instalar programas para restringir la navegación por determinados sitios web o para controlar qué páginas visitan los empleados o los correos que envían y reciben.

26. En tu empresa acaban de crear unas claves de seguridad para los empleados. Dichas claves se envían por correo electrónico. ¿Esto es desconocimiento de las prácticas de seguridad?

Sí, porque las contraseñas nunca deben enviarse por correo electrónico.

ACTIVIDADES-PÁG. 23

27. El hecho de preparar un plan de contingencias, ¿implica un reconocimiento de la ineficiencia en la gestión de la empresa?

No. Supone un importante avance a la hora de superar todas aquellas situaciones (problema informático, fallo en la correcta circulación de información o falta de provisión de servicios básicos tales como energía eléctrica, gas, agua y telecomunicaciones) que pueden provocar importantes pérdidas, no solo materiales sino aquellas derivadas de la paralización del negocio durante un período más o menos largo.

28. ¿Cuál es la orientación principal de un plan de contingencia?

La continuidad de las operaciones de la empresa.

29. Investiga: diferencias entre redes cableadas y redes inalámbricas WIFI.

- **Cableadas.** La información se envía por cable –que es un medio privado– y mediante señales eléctricas.
- **WIFI.** La información se transmite por el aire –que es un medio público y compartido– mediante ondas de radio frecuencia.

30. ¿En qué se basa la recuperación de la información?

En una correcta política de copias de seguridad.

31. Tu jefe te pide que le hagas una buena política de copias de seguridad para que sea seguida por todos los trabajadores de la empresa. ¿Qué deberá contemplar?

Con los conocimientos adquiridos hasta ahora, la respuesta no ha de profundizar necesariamente en el tema. No obstante, si se investiga y se razona, se puede deducir que normalmente una política de copias de seguridad contendrá como mínimo:

- Indicación del tipo de copias que han de hacerse: completas o solamente agregando los datos nuevos (copias incrementales).
- Indicación de la frecuencia con que se han de realizar las copias de seguridad.
- Cuántas copias de seguridad deben tenerse.
- En qué lugar se deben guardar.

32. Trabajas en una empresa donde además de la oficina central, hay una red de oficinas por varias ciudades. Se elabora un plan de contingencias exclusivamente para la oficina central, ¿es esto correcto?

No. El plan de contingencias deberá abarcar a toda la empresa.

33. En tu empresa se desarrolla un plan de contingencias que entre otras muchas situaciones, cubre las siguientes: un corte en la corriente eléctrica, el sol pasando a través de un cristal en pleno agosto, derramar una bebida en el teclado o sobre el monitor, olvidarse el portátil en un taxi, el robo del ordenador. ¿Crees que cubrir estos puntos es acertado?

Sí.

ACTIVIDADES-PÁG. 24

34. ¿Una misma política de seguridad puede servir a todo tipo de empresas?

No. La política de seguridad tiene que basarse en la realidad y en las necesidades de cada empresa.

35. ¿De qué modo debe ser redactada la política de seguridad de una organización?

De modo que pueda ser comprendida por todo el personal de la organización.

36. Define con tus propias palabras qué es un plan de contingencias.

Definición personal.

37. Investiga en internet sobre empresas especializadas en auditorías de sistemas de información (sugerencias: Hipasec, Audisis). Escoge una de estas empresas y contesta las siguientes preguntas:

a) ¿En qué fases realiza la auditoría?
b) ¿Qué tipos de auditoría realiza?
c) ¿Ofrece revisiones periódicas del sistema?

Respuesta personal en función de las empresas auditoras que localicen y de la información que tengan expuesta en internet (o en cualquier otra fuente) en el momento de la búsqueda.

38. Investiga en internet para encontrar el software de auditoría: CaseWare, WizSoft, Ecora, ACL, AUDAP u otros. Escoge uno o varios y haz una lista de las operaciones que realiza para llevar a cabo la auditoría.

Respuesta personal que depende del software analizado y de lo que esté publicado en ese momento en internet.

39. Averigua qué información tiene wikipedia sobre el modelo de seguridad Bell-LaPadula. Escribe la definición que hace del modelo.

En seguridad informática, el modelo de seguridad Bell-LaPadula, llamado así por sus creadores David Elliott Bell y Len LaPadula, consiste en dividir el permiso de acceso de los usuarios a la información en función de etiquetas de seguridad.

Por ejemplo, en sistemas militares norteamericanos, categorizándola en 4 niveles: no clasificado, confidencial, secreto y ultra secreto.

PRÁCTICA PROFESIONAL-PÁG. 25

Con los conocimientos que posees tras haber estudiado esta unidad:

1. Enumera los activos del sistema de información de la asesoría.

La ubicación física de la asesoría con todas sus habitaciones.
5 ordenadores y un servidor.
1 portátil.
1 impresora.
1 escáner.
Archivo o armario para guardar las copias de seguridad.
Copias de seguridad.
1 mesa de reuniones.
Sillas.
Proyector.
Pantalla.
5 personas.
Sistemas operativos y software.
Información.

2. ¿Se ha producido algún ataque? En caso afirmativo responde cuál ha sido.

Sí. Un pico de corriente ha estropeado la placa base y el disco duro del ordenador de dirección.

3. ¿Crees que ha sido importante para la empresa el impacto por los daños en la placa base y el disco duro? Comenta tu impresión.

La sustitución del disco duro y de la placa base no es costosa. Existía una copia de seguridad de los datos perdidos. Por tanto el impacto es pequeño.

4. Investiga si existe algún medio para evitar que los picos de corriente puedan dañar equipos o dispositivos físicos de un sistema informático.

Sí, hay sistemas de alimentación ininterrumpida o también simples estabilizadores de corriente.

5. El disco duro inutilizado contenía información personal y fiscal de clientes de la asesoría. Se ha decidido tirarlo a la basura, pero una empleada dice que ese método no es seguro. Haz tus investigaciones y comenta si has averiguado que la empleada está o no en lo cierto.

Un disco duro incluso estropeado o formateado, mediante técnicas especiales puede ofrecer aún información de su contenido, total o incompleta. La empleada está en lo cierto.

MUNDO LABORAL-PÁG. 26

Lee el artículo y en vista de su contenido responde a las siguientes cuestiones:

1. **¿Qué propiedades de seguridad del sistema de información podrían verse vulneradas por negligencias cometidas por empleados de la empresa al publicar sus datos personales en redes sociales?**

   Todas: la confidencialidad, la integridad y la disponibilidad.

2. **Indica alguna manera en que los administradores de un sistema de información pueden impedir que el personal de la empresa acceda a sitios que podrían poner en peligro las propiedades de seguridad del sistema.**

   Mediante una política de seguridad, con la formación del personal de la empresa y mediante programas de control y limitación de acceso a determinados sitios de internet.

3. **¿Qué proporción de negocios se ven afectados por *spam* o software malicioso debido al uso indebido de redes sociales por parte de los empleados?**

   Una cuarta parte.

4. **En tu opinión, ¿consideras cierta la afirmación de que se producen más fallos de seguridad por la intervención humana que por errores en la tecnología?**

   Está claro que sí.