

Práctica RA1

Pol de la Viuda

Contenido

Caso 1	3
Enumera los activos del sistema de información de la asesoría.....	3
¿Se ha producido algún ataque? En caso afirmativo, responde cuál ha sido.	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.	3
Investiga si existe algún medio para evitar que los picos de corriente puedan dañar equipos o dispositivos físicos de un sistema informático.	3
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 la empleada está o no en lo cierto.	4
¿Qué medidas de seguridad física y lógica podrían reforzarse en la empresa para evitar incidentes similares en el futuro?	4
¿Si la copia de seguridad diaria también se hubiera dañado, qué consecuencias legales y operativas podría tener para la asesoría?.....	4
Imagina que eres el responsable de seguridad informática de la empresa:	4
Caso 2.....	5
¿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?	5
Indica alguna manera de que los administradores de un sistema de información puedan impedir que el personal de la empresa acceda a sitios que podrían poner en peligro las propiedades de seguridad del sistema.	5
¿Qué proporción de negocios se ven afectados por spam o software malicioso debido al uso indebido de redes sociales por parte de los empleados?	5
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?	6
Si trabajas en una empresa, ¿crees que deberías tener libertad total para usar tus redes sociales desde el trabajo, o aceptarías ciertas restricciones de seguridad? ¿Por qué?.....	6
¿Qué medidas de formación o concienciación podrían aplicarse para reducir los riesgos humanos en ciberseguridad dentro de una empresa?	6
Imagina que un compañero publica información laboral confidencial sin darse cuenta. ¿Cómo actuarías tú y qué protocolo debería seguir la empresa en ese caso?	6

Caso 1

Enumera los activos del sistema de información de la asesoría.

- 4 ordenadores
- 1 servidor
- Una impresora
- Un escáner
- Un portátil
- Una pantalla
- Un proyector
- 5 trabajadores

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

No se ha producido ningún ataque, el problema tiene que ver con un pico de corriente, que ha generado daños en la placa base y el disco duro

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

Yo creo que no ha sido muy importante, ya que solo tienen que cambiar los componentes, ya que hacen copias de seguridad y no han perdido datos

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

Los picos de corriente se pueden evitar con un sistema de alimentación ininterrumpida, ya que esto protege a los equipos contra picos, cortes y variaciones de tensión

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 la empleada está o no en lo cierto.

La empleada esta en lo cierto, ya que por mas que el disco duro este dañado, tiene la información dentro y todavía se puede recuperar de alguna forma

¿Qué medidas de seguridad física y lógica podrían reforzarse en la empresa para evitar incidentes similares en el futuro?

Para mejorar la seguridad física de la empresa, se podrían instalar sistemas de alimentación ininterrumpida para evitar mas problemas como el que ya ha ocurrido y en cuanto a medidas lógicas, lo tienen muy bien ya que tienen unas políticas de seguridad que las conoce todo el personal, y tienen copias de seguridad automatizadas

¿Si la copia de seguridad diaria también se hubiera dañado, qué consecuencias legales y operativas podría tener para la asesoría?

Si se hubiera dañado, la asesoría hubiera tenido muchas consecuencias, ya que hubiesen perdido todos los datos y toda la información que tenían y para la hora de trabajar les costaría mucho sin esa información, y en cuanto tema legal podrían tener sanciones económicas por la agencia español de protección de datos, según el artículo que habla sobre el principio de integridad y confidencialidad, que habla sobre todo este tema de perdida de datos confidenciales

[Link del articulo](#)

Imagina que eres el responsable de seguridad informática de la empresa:

¿Qué plan de acción implementarías tras este incidente para mejorar la protección de los equipos y los datos?

Instalaría sistemas de alimentación ininterrumpidos para evitar todo tipo de problemas con la electricidad y proteger los equipos de los problemas que ya han ocurrido

Caso 2

¿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?

El primero y más obvio es la confidencialidad, ya que si subes algo relacionado con la empresa se pueden ver cosas privadas que no se deberían ver, ya pueden ser datos o contraseñas

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

Hay varias formas, pero las que yo creo que servirán mejor son las siguientes

Bloquear el acceso a redes sociales o sitios sospechosos mediante firewalls, proxys o filtros de contenido

Implementar sistemas de detección y prevención de intrusos

Usar listas negras (blacklists) de sitios peligrosos y listas blancas (whitelists) con sitios permitidos

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

Según el informe de Sophos, una cuarta parte de los negocios les afecta el spam, el phishing o ataques de software maliciosos

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?

Yo creo que sí que es cierta, ya que hay mucha gente que trabaja en empresas que les falta mucho conocimiento sobre este tema y la gente que no sabe sobre el tema tampoco intenta aprender cosas para evitar problemas, lo que deberían hacer las empresas es hacer más cursos sobre seguridad para el bien de la empresa

Si trabajas en una empresa, ¿crees que deberías tener libertad total para usar tus redes sociales desde el trabajo, o aceptarías ciertas restricciones de seguridad? ¿Por qué?

Yo creo que no deberías tener libertad total, ya que hay cosas de la empresa que la gente no debería ver y si los subes públicamente lo puede ver quien quiera, como por ejemplo te puede sacar una foto con un compañero de trabajo y que de fondo se vea una contraseña o algún dato importante de la empresa, entonces para evitar esto se deberían de poner restricciones

¿Qué medidas de formación o concienciación podrían aplicarse para reducir los riesgos humanos en ciberseguridad dentro de una empresa?

Para reducir los riesgos humanos, la empresa debería obligar a los trabajadores a hacer un curso sobre ciberseguridad y que los trabajadores se lo tomen en serio, y que hagan algún curso mas online en su casa para tener mas conocimiento sobre el tema

Imagina que un compañero publica información laboral confidencial sin darse cuenta. ¿Cómo actuarías tú y qué protocolo debería seguir la empresa en ese caso?

Primero le diría al compañero que borrara lo que ha subido ya que se ve información confidencial que no se puede ver, si lo que se ve no es muy grave se le tendría que dar un toque de atención pero si lo que se ve puede afectar negativamente a la empresa se debería de despedir al trabajador