SEGURIDAD INFORMÁTICA

Contenido

Ejercicio 1.

En términos ideales la seguridad informática sería la cualidad de un sistema informático libre y exento de todo peligro, daño o riesgo. Sin embargo, un sistema informático en explotación, al que acceden usuarios, no puede satisfacer dicha definición. Así pues, la seguridad informática no puede ser un producto porque es un objetivo inalcanzable. Hay que ver la seguridad informática como un proceso permanente cuya finalidad es proteger los activos informáticos. ¿Cuáles son estos activos informáticos?

- Hardware (equipos, servidores, redes, dispositivos de almacenamiento).
- Software (sistemas operativos, aplicaciones, servicios).
- Datos e información (archivos, bases de datos, conocimiento de la organización).
- Recursos humanos (usuarios, administradores, técnicos).
- Infraestructura y servicios (electricidad, comunicaciones, Internet).

Ejercicio 2.

Con respecto a la información manejada, ¿qué tres aspectos se deben garantizar?

- Confidencialidad → Solo las personas autorizadas acceden a la información.
- Integridad → La información no se altera de manera indebida.
- Disponibilidad → La información y sistemas están accesibles cuando se necesitan.

Ejercicio 3.

En cuanto a la infraestructura computacional, ¿por qué se debe velar?

- Por su funcionamiento continuo, evitando interrupciones.
- Por su protección física (incendios, inundaciones, robos).
- Por su resiliencia (mantenimiento, respaldo eléctrico, redundancia).

Ejercicio 4.

A los usuarios hay que protegerlos, ¿de qué tipos de daños?

- Daños físicos (corrientes eléctricas, ergonomía, incendios).
- Daños psicológicos o sociales (fraudes, phishing, acoso digital).
- Daños económicos (robo de identidad, estafas).

Ejercicio 5.

Los activos pueden ser afectados por circunstancias fortuitas o deliberadas. Estas circunstancias, que constituyen una violación potencial de la seguridad, se denominan...

- Amenazas.

Ejercicio 6.

La seguridad no es un producto, sino un proceso permanente que tiene que estar integrado en los procesos cotidianos de la estructura institucional y que debe incluir a todos los miembros de dicha estructura. Dicho proceso se puede dividir, ¿en qué fases?

- Análisis (identificación de activos, amenazas y vulnerabilidades).
- Clasificación de riesgos (valoración de probabilidad e impacto).
- Planificación y selección de medidas.

- Implementación de medidas.
- Supervisión y mejora continua.

Ejercicio 7.

Una organización después de realizar el análisis de la seguridad desea realizar un plan de acción para reducir su inseguridad informática (fase de clasificación). La organización ha identificado varias amenazas: intrusión, incendio, inundación, virus, sismo, robo, sabotaje, espionaje, fallo eléctrico y negligencia. A cada amenaza, teniendo en cuenta las vulnerabilidades del sistema, se le ha asignado una probabilidad entre 0 y 10 de causar impacto. Dichas probabilidades son, respectivamente: 4, 2, 1, 4, 1, 2, 3, 2, 2 y 5. Para cada amenaza también se ha estimado el impacto entre 0 y 10, siendo dichas estimaciones las siguientes: 6, 9, 8, 5, 8, 7, 4, 5, 2 y 2. A partir de la probabilidad y del impacto se obtiene el factor de riesgo multiplicándolos. Para cada amenaza se ha estimado el coste entre 10 y 0 de las medidas a tomar para prevenirla. Estos valores se han estimado al inverso de lo habitual, es decir, un coste 9 es un coste bajo y un coste 1 es un coste alto. Dichos valores estimados son los siguientes: 6, 3, 3, 6, 1, 7, 5, 5, 8 y 8. Finalmente, para cada amenaza se obtiene un factor de prioridad, es decir, cual es la amenaza para la que se deberían tomar medidas en primer lugar. El factor de prioridad se obtiene multiplicando el factor de riesgo por el coste de las medidas a tomar. Realizad una hoja Excel que muestre claramente todos los datos anteriores ordenados por factor de prioridad decreciente. La hoja de cálculo realizada hay que insertarla como vínculo en el documento de Word. La hoja Excel se insertará en Word en una página apaisada mientras que las páginas anteriores y posteriores no lo son.

Amenaza	Probabilidad	Impacto	Riesgo	Coste	Prioridad
Intrusión	4	6	24	6	144
Incendio	2	9	18	3	54
Inundación	1	8	8	3	24
Virus	4	5	20	6	120
Sismo	1	8	8	1	8
Robo	2	7	14	7	98
Sabotaje	3	4	12	5	60
Espionaje	2	5	10	5	50
Fallo eléctrico	2	2	4	8	32
Negligencia	5	2	10	8	80

Intrusión (144) - Virus (120) - Robo (98) - Negligencia (80) - Sabotaje (60) - Incendio (54) - Espionaje (50) - Fallo eléctrico (32) - Inundación (24) - Sismo (8)

Ejercicio 8.

La reducción de riesgos se logra a través de la implementación de medidas de protección que se basen en los resultados del análisis y de la clasificación de riesgo. Enfoques tradicionales del estudio de la seguridad clasificaban estas medidas en dos tipos, ¿qué son?

- Medidas preventivas (evitar que ocurra el daño).
- Medidas reactivas/correctivas (minimizar el impacto una vez ocurrido).

Ejercicio 9.

Finalmente hay que decir que estos enfoques están evolucionando por varios motivos. Uno de ellos es que cada vez está menos claro dónde termina la seguridad física y la lógica. Por otro lado, la seguridad suele considerarse como una cuestión tecnológica pero básicamente comporta problemas organizativos y específicamente humanos, es decir, son necesarias

medidas organizativas de seguridad. Estas medidas organizativas de seguridad se suelen englobar en...

- Políticas de seguridad (normas, roles, responsabilidades).
- Procedimientos operativos.
- Formación y concienciación de usuarios.
- Planes de contingencia y continuidad de negocio.

Bibliografía y enlaces.

Bibliografía y enlaces.