Comenzado el	martes, 23 de noviembre de 2021, 11:13
Estado	Finalizado
Finalizado en	martes, 23 de noviembre de 2021, 11:34
Tiempo empleado	21 minutos 4 segundos
Calificación	**4,10** de 5,00 (**82**%)
Comentario -	La retroalimentación de la evaluación se habilitará cuando la docente haya verificado que todos los estudiantes finalizaron con el cuestionario.

Pregunta **1**

Correcta

Se puntúa 1,00 sobre 1,00

Considerando la administración del riesgo, asocie cada ejemplo con el concepto que corresponde.

El oficial de seguridad de la información constantemente revisa reportes de vulnerabilidades y amenazas que son publicados en registros oficiales. ✔ — Conocer al enemigo

Una organización ha detectado que no realiza actualizaciones frecuentes de los sistemas operativos de sus servidores. ✔ — Localización de debilidades

Una empresa que vende productos en línea tiene una probabilidad de un 40% de que su servidor web sea víctima de un ataque. ✔ — Riesgo involucrado

El personal a cargo de la seguridad de la información identifica los controles existentes. ✔ — Comprender cómo están actualmente protegidos

Respuesta correcta

La respuesta correcta es:
El oficial de seguridad de la información constantemente revisa reportes de vulnerabilidades y amenazas que son publicados en registros oficiales. → Conocer al enemigo,

Una organización ha detectado que no realiza actualizaciones frecuentes de los sistemas operativos de sus servidores. → Localización de debilidades,

Una empresa que vende productos en línea tiene una probabilidad de un 40% de que su servidor web sea víctima de un ataque. → Riesgo involucrado,

El personal a cargo de la seguridad de la información identifica los controles existentes. → Comprender cómo están actualmente protegidos

Pregunta **2**

Parcialmente correcta

Se puntúa 0,75 sobre 1,00

Asocie cada ejemplo con la amenza que corresponde:

Un empleado de la organización descarga un malware que recibió como archivo adjunto en un correo. — Robo ✖

Uno de los servidores de la organización cuenta con un sistema operativo para el cual se suspenderá el soporte a mediados de año. — Obsolecescencia tecnológica ✔

Un empleado que ha renunciado para trabajar con la competencia, accede a la base de datos de clientes, genera una copia de los datos y se lleva esa información. — Espionaje o allanamiento ✔

Debido a variaciones de voltaje, el disco duro de uno de los servidores de la organización se quema. — Fallos técnicos o errores de hardware ✔

Respuesta parcialmente correcta.

Ha seleccionado correctamente 3.
La respuesta correcta es:

Un empleado de la organización descarga un malware que recibió como archivo adjunto en un correo. → Errores humanos o fallas,

Uno de los servidores de la organización cuenta con un sistema operativo para el cual se suspenderá el soporte a mediados de año. → Obsolecescencia tecnológica,

Un empleado que ha renunciado para trabajar con la competencia, accede a la base de datos de clientes, genera una copia de los datos y se lleva esa información. → Espionaje o allanamiento,

Debido a variaciones de voltaje, el disco duro de uno de los servidores de la organización se quema. → Fallos técnicos o errores de hardware

Pregunta **3**

Parcialmente correcta

Se puntúa 0,60 sobre 1,00

Asocie cada ejemplo presentado con el término que corresponde.

Un servidor web. — Activo ✔

Un informe de la compañía de seguridad Kaspersky señaló que el 27% de los empleados que trabajan de manera remota recibieron correos electrónicos de phishing relacionados con el coronavirus. — Riesgo ✔

Micrsoft ha reportado que los sistemas operativos Windows 7, 8.1, RT 8.1, 10, Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019 pueden ser víctimas de ejecución remota de código que afecta a la biblioteca Adobe Type Manager. — Amenaza ✖

Una organización ha sido víctima de ingeniería social y los registros de datos de sus clientes fueron robados. — Ataque ✔

Cuando una empresa no cuenta con políticas sobre el manejo de usuarios y contraseñas. — Vulnerabilidad ✖

Respuesta parcialmente correcta.

Ha seleccionado correctamente 3.
La respuesta correcta es:
Un servidor web. → Activo,

Un informe de la compañía de seguridad Kaspersky señaló que el 27% de los empleados que trabajan de manera remota recibieron correos electrónicos de phishing relacionados con el coronavirus. → Riesgo,

Micrsoft ha reportado que los sistemas operativos Windows 7, 8.1, RT 8.1, 10, Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019 pueden ser víctimas de ejecución remota de código que afecta a la biblioteca Adobe Type Manager. → Vulnerabilidad,

Una organización ha sido víctima de ingeniería social y los registros de datos de sus clientes fueron robados. → Ataque,

Cuando una empresa no cuenta con políticas sobre el manejo de usuarios y contraseñas. → Amenaza

Pregunta **4**

Correcta

Se puntúa 1,00 sobre 1,00

A fin de desarrollar un criterio de valoración para activos de información, determine si las siguentes afirmaciones son verdaderas o falsas.

Todos los activos de la organización deben considerarse como críticos. — Falso ✔

Para una empresa que vende productos en línea, se puede considerar que su servidor web genera más ingresos que su servidor de correo electrónico. — Verdadero ✔

La pérdida o compromiso de los activos se evalúa únicamente en términos monetarios. — Falso ✔

Se deberán aplicar medidas de protección para los activos siempre y cuando no sean caros de protegerlos. — Falso ✔

Respuesta correcta

La respuesta correcta es:
Todos los activos de la organización deben considerarse como críticos. → Falso,

Para una empresa que vende productos en línea, se puede considerar que su servidor web genera más ingresos que su servidor de correo electrónico. → Verdadero,

La pérdida o compromiso de los activos se evalúa únicamente en términos monetarios. → Falso,

Se deberán aplicar medidas de protección para los activos siempre y cuando no sean caros de protegerlos. → Falso

Pregunta **5**

Parcialmente correcta

Se puntúa 0,75 sobre 1,00

Considerando el análisis y evaluación del riesgo, indique si las siguientes afirmaciones son verdaderas o falsas.

Las organizaciones implementan controles de seguridad únicamente luego de haber realizado un análisis y evaluación del riesgo. — Verdadero ✖

No siempre se debe reducir el riesgo residual. — Verdadero ✔

Se puede reducir el riesgo a un 0% si se implementan los controles de seguridad adecuados. — Falso ✔

La programas son controles innecesarios si ya se cuenta con políticas de seguridad dentro de la organización. — Falso ✔

Respuesta parcialmente correcta.

Ha seleccionado correctamente 3.
La respuesta correcta es:
Las organizaciones implementan controles de seguridad únicamente luego de haber realizado un análisis y evaluación del riesgo. → Falso,

No siempre se debe reducir el riesgo residual. → Verdadero,

Se puede reducir el riesgo a un 0% si se implementan los controles de seguridad adecuados. → Falso,

La programas son controles innecesarios si ya se cuenta con políticas de seguridad dentro de la organización. → Falso

Actividad previa | Ir a... | Próxima actividad