# SEGURIDAD DE LA INFORMACIÓN GRUPO - 1

| | |
|---|---|
| **Comenzado el** | martes, 30 de noviembre de 2021, 11:11 |
| **Estado** | Finalizado |
| **Finalizado en** | martes, 30 de noviembre de 2021, 11:51 |
| **Tiempo empleado** | 39 minutos 54 segundos |
| **Calificación** | **5,65** de 10,00 (**56**%) |
| **Comentario -** | La retroalimentación se habilitará cuando la docente haya verificado que todos los estudiantes cumplieron con la evaluación. |

Pregunta **1**

Parcialmente correcta

Puntúa 0,83 sobre 1,25

Marcar pregunta

Complete el siguiente texto con los términos correctos.

La Ley Orgánica de Protección de Datos aprobada en Ecuador constituye [un estándar] ✗ que se encarga de regular el tratamiento de los datos personales en Ecuador. Para proteger los datos es importante clasificarlos considerando [metadatos] ✓ como fecha en la que se generaron los datos, propietarios, formatos, entre otros. Es así que, contar con un esquema de clasificación de información permitirá contar con [confidencialidad] ✓ a fin de asegurar que solo las personas autorizadas tienen acceso a los datos.

Pregunta **2**

Parcialmente correcta

Puntúa 0,75 sobre 1,00

Marcar pregunta

Considerando que se debe identificar y priorizar las amenazas y agentes de amenazas, indique si las siguientes afirmaciones son verdaderas o falsas.

La amenaza de daño o destrucción de los sistemas de información es igual de peligrosa tanto para un supermercado local como para un banco nacional. — Falso ✓

Considerando las categorías de amenazas para InfoSec publicado en JISSec, es importante que las organizaciones identifiquen al menos una amaneza para cada categoría. — Falso ✓

Un ataque de suplantación de identidad ocurre con la misma frecuencia para un hospital que para un banco. — Falso ✓

El peligro asociado a una amenaza siempre debe ser valorado de manera cuantitativa porque de esa manera puede ser evaluado fácilmente. — Verdadero ✗

Respuesta parcialmente correcta.

Ha seleccionado correctamente 3.
La respuesta correcta es:
La amenaza de daño o destrucción de los sistemas de información es igual de peligrosa tanto para un supermercado local como para un banco nacional. → Falso,

Considerando las categorías de amenazas para InfoSec publicado en JISSec, es importante que las organizaciones identifiquen al menos una amaneza para cada

Pregunta **3**

Incorrecta

Puntúa 0,00 sobre 2,00

Marcar pregunta

Considerando la fórmula:

Riesgo = (Valor del Activo de Información * Probabilidad de ocurrencia de la vulnerabilidad) - % riesgo mitigado + % incertidumbre de la vulnerabilidad

Calcule el riesgo para los activos A, B y C.

- El activo de información A tiene un valor de 70, con una vulnerabilidad A1 que tiene una probabilidad de ocurrencia del 0.9. Se aplican controles que dejan un riesgo remanente del 15% y cuya incertidumbre alcanza el 30%.
- El activo de información B tiene un valor de 95 expuesto a una vulnerabilidad B1, cuya probabilidad de ocurrencia es del 0.5. Se aplican controles para abordar el 40% del riesgo, con una precisión de supuestos del 80%.
- El activo de información C tiene un valor de 92, con una vulnerabilidad C1 que cuenta con una probabilidad de ocurrencia del 0.6. Luego de los controles queda un riesgo del 30% y la precisión de los supuestos es del 78%.

Activo A - Vulnerabilidad A1

Riesgo = 24.5 ✖

Activo B - Vulnerabilidad B1

Riesgo = 28.5 ✖

Activo C - Vulnerabilidad C1

Riesgo = 11.04 ✖

Pregunta **4**

Correcta

Puntúa 1,25 sobre 1,25

Marcar pregunta

Asocie cada ejemplo con el tipo de información que corresponde.

| | |
|---|---|
| Código fuente del sistema operativo Windows. | Información correspondiente a un secreto comercial ✔ |
| Información sobre la localización y el control de los misiles nucleares de un país. | Información de seguridad nacional ✔ |
| Los datos de localización del celular de una persona. | Información personal ✔ |
| El estado financiero y de presupuesto anual de una empresa del estado. | Información pública ✔ |

Respuesta correcta

La respuesta correcta es:
Código fuente del sistema operativo Windows. → Información correspondiente a un secreto comercial,

Información sobre la localización y el control de los misiles nucleares de un país. → Información de seguridad nacional,

Los datos de localización del celular de una persona. → Información personal,

El estado financiero y de presupuesto anual de una empresa del estado. → Información pública

Pregunta **5**

Parcialmente correcta

Puntúa 0,94 sobre 1,25

Marcar pregunta

Considerando los retos de Seguridad de la Información indique si las siguientes afirmaciones son verdaderas o falsas.

Si una organización cuenta con una guía que detalla cómo se debe destruir los documentos físicos que tienen más de 5 años de antigüedad, se puede concluir que la organización aplica medidas de ciberseguridad. — Falso ✔

El equipo de desarrollo de una organización ha decidido aplicar prácticas de código seguro desde el inicio del proyecto; por lo tanto, se puede concluir que habrán retrasos en el cumplimiento del cronograma. — Falso ✔

Hoy en día un actor de amenaza requiere mucho conocimiento para poder elaborar un ataque hacia una organización objetivo. — Verdadero ✖

Cuando se implementan medidas de seguridad de la información se debe encontrar un balance entre seguridad y disponibilidad de los servicios. — Verdadero ✔

Respuesta parcialmente correcta.

Ha seleccionado correctamente 3.
La respuesta correcta es:
Si una organización cuenta con una guía que detalla cómo se debe destruir los documentos físicos que tienen más de 5 años de antigüedad, se puede concluir que la organización aplica medidas de ciberseguridad. → Falso,

El equipo de desarrollo de una organización ha decidido aplicar prácticas de código seguro desde el inicio del proyecto; por lo tanto, se puede concluir que habrán retrasos en el cumplimiento del cronograma. → Falso,

Hoy en día un actor de amenaza requiere mucho conocimiento para poder elaborar un ataque hacia una organización objetivo. → Falso,

Cuando se implementan medidas de seguridad de la información se debe encontrar un balance entre seguridad y disponibilidad de los servicios. → Verdadero

Pregunta **6**

Parcialmente correcta

Puntúa 0,75 sobre 1,00

Marcar pregunta

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

La empresa debe determinar si su infraestructura está expuesta a riesgos naturales debido a su ubicación geográfica. — Conociéndose a sí mismo ✔

Deben asegurar que una aplicación web sea desarrollada siguiendo buenas prácticas para el desarrollo de código seguro. — Gerentes de TI ✔

Pueden ser los primeros en descargar un malware que recibieron como adjunto en un correo electrónico. — Gerentes y usuarios ✔

La organización determina que su servidor de base de datos está expuesto a la amenaza de denegación de servicio. — Gerentes de InfoSec ✖

Respuesta parcialmente correcta.

Ha seleccionado correctamente 3.
La respuesta correcta es:
La empresa debe determinar si su infraestructura está expuesta a riesgos naturales debido a su ubicación geográfica. → Conociéndose a sí mismo,

Deben asegurar que una aplicación web sea desarrollada siguiendo buenas prácticas para el desarrollo de código seguro. → Gerentes de TI,

Pueden ser los primeros en descargar un malware que recibieron como adjunto en un correo electrónico. → Gerentes y usuarios,

La organización determina que su servidor de base de datos está expuesto a la amenaza de denegación de servicio. → Conociendo al enemigo

Puntúa 0,50 sobre 1,00

Marcar pregunta

Los empleados no actualizan sus contraseñas de acceso al sistema organizacional, cada tres meses, como indica la política de seguridad. — Errores humano o fallas ✔

La empresa eléctrica de la ciudad en la que está ubicada una de las sucursales de una organización realizará cortes de energía por el lapso de una semana (2 horas por día). — Desviaciones en la calidad del servicio de los proveedores de servicios ✔

El gerente de un banco que fue víctima de un ataque de filtración de datos recibió un correo electrónico solicitando dinero a cambio de no publicar toda la información que fue robada. — Ataques de software ✖

Una persona no autorizada puede acceder al sistema de una organización. — Errores humano o fallas ✖

Respuesta parcialmente correcta.

Ha seleccionado correctamente 2.
La respuesta correcta es:
Los empleados no actualizan sus contraseñas de acceso al sistema organizacional, cada tres meses, como indica la política de seguridad. → Errores humano o fallas,

La empresa eléctrica de la ciudad en la que está ubicada una de las sucursales de una organización realizará cortes de energía por el lapso de una semana (2 horas por día). → Desviaciones en la calidad del servicio de los proveedores de servicios,

El gerente de un banco que fue víctima de un ataque de filtración de datos recibió un correo electrónico solicitando dinero a cambio de no publicar toda la información que fue robada. → Extorsión de información,

Una persona no autorizada puede acceder al sistema de una organización. → Fallos técnicos o errores de software

Pregunta **8**

Parcialmente correcta

Puntúa 0,63 sobre 1,25

Marcar pregunta

Al clasificar los datos, deben tenerse en cuenta algunos requisitos. Asocie cada ejemplo con el requisito que corresponde.

Los roles de pago deben ser ser generados y modificados únicamente por la contadora general de la organización. — Privacidad ✖

Una banca virtual debe ser accesible a sus clientes 24x7. — Disponibilidad ✔

De acuerdo a una política organizacional, los datos deben almacenarse por al menos 3 años. — Retención de datos ✔

El personal de recursos humanos debe acceder a la información de los empleados y sus contratos; pero no debe tener acceso a la información del inventario de activos. — Integridad ✖

Respuesta parcialmente correcta.

Ha seleccionado correctamente 2.
La respuesta correcta es:
Los roles de pago deben ser ser generados y modificados únicamente por la contadora general de la organización. → Integridad,

Una banca virtual debe ser accesible a sus clientes 24x7. → Disponibilidad,

De acuerdo a una política organizacional, los datos deben almacenarse por al menos 3 años. → Retención de datos,

El personal de recursos humanos debe acceder a la información de los empleados y sus contratos; pero no debe tener acceso a la información del inventario de activos. → Acceso y autenticación