

SEGURIDAD INFORMÁTICA I

Cuestionario

# Alumno: Lucas Damián Soria Gava

# Legajo: 58156

# PREGUNTAS

X - - - - - - - - - - - - - - - - - - - - - - - - - - - - X

1. ¿Los Datos me ayudan en una Decisión?
2. ¿Los Datos conforman la sabiduría?
3. ¿Sin Información no logramos el objetivo?
4. ¿El Riesgo es el daño sobre el activo?
5. ¿Cuántos pasos son necesarios para implementar la seguridad informática?
6. ¿Cual es el comienzo y el final de PDCA?
7. Mencione un activo duro, soft, físico, intangible, tangible
8. ¿Un ACTIVO puede tener valor cero?
9. ¿A que se le denomina IMPACTO a un ACTIVO?
10. ¿Cómo crece el RIESGO?
11. ¿Las SALVAGUARDAS son o no las CONTRAMEDIDAS?
12. ¿Para asegurar la DISPONIBILIDAD, CONFIDENCIALIDAD e INTEGRIDAD es necesario gestionar al personal?
13. ¿El Dominio 8 de la ISO 27001 y 27002 que trata?
14. ¿Qué se propone con la ISO-IEC 71?
15. Clase de Controles Internos
16. ¿Que se propone con la GESTIÓN DE LOS ACTIVOS?
17. ¿La GESTIÓN INTEGRAL DE SEGURIDAD incluye que temas?
18. Cada ACTIVO tiene 3 propiedades
19. ¿La GESTIÓN DE LA SEGURIDAD está a cargo de quienes en la EMPRESA?

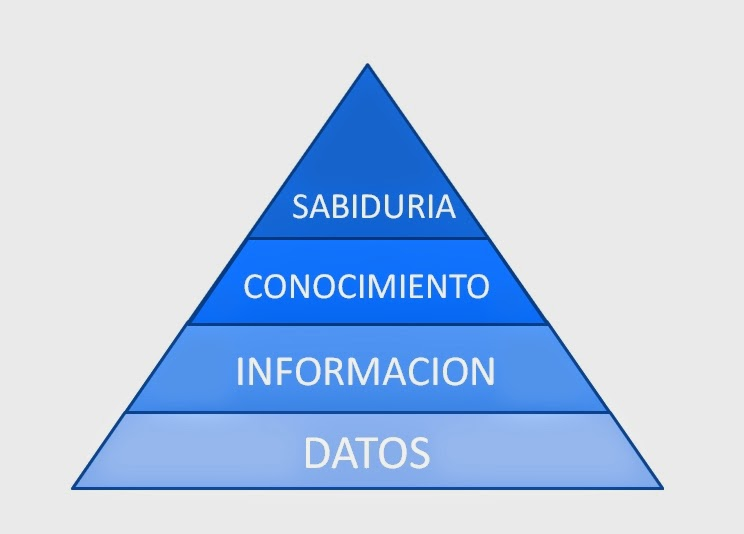
# RESPUESTAS

X - - - - - - - - - - - - - - - - - - - - - - - - - - - - X

1. Los datos son la representación simbólica de una variable (cuantitativa o cualitativa). Los datos ayudan en la toma de decisiones porque son los datos los que nos permiten tomar decisiones informadas, las cuales se toman a partir de un pensamiento crítico. Estas decisiones son las que nos permiten llegar al objetivo que nos planteemos. Los datos también permiten fundamentar nuestras decisiones y acciones.

El valor del sistema de información se centra en los datos que maneja, ya que este es su activo esencial.

1. Los datos conforman la información, a partir de ella podemos generar conocimiento y a partir de este podemos obtener sabiduría. Esto es así porque la información es aquello que se extrae de un conjunto de datos, el conocimiento lo que se genera a partir del análisis de la información, y la sabiduría es el producto de acumular conocimiento y experiencia.



1. Si bien es posible lograr nuestros objetivos sin información, esta forma de operar no garantiza lograr nuestro siguiente objetivo, de hecho, se puede afirmar que lograr nuestros objetivos sin información es casualidad.

La información nos permite tomar decisiones y estas guían nuestras acciones. Las acciones que tomamos a partir de decisiones informadas son las que nos permiten lograr nuestros objetivos.

1. El Riesgo es la medida del daño probable sobre un sistema. El riesgo se valora a través de la multiplicación entre la probabilidad de una amenaza y la magnitud del daño que esta pueda causar. Este crece con el impacto que tiene una amenaza sobre los activos y con la frecuencia con la que se presenta.
2. Para implementar la seguridad informática se necesitan 4 pasos: Planificar, hacer, verificar y actuar.
3. El comienzo del PDCA es la planificación, donde se define el ​alcance​ ​del SGSI (Sistema de Gestión de la Seguridad de la información) en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión. Y el final es el actual, donde se implementan en el SGSI las mejoras identificadas y se realizan y comunican acciones preventivas o correctivas.

Sin embargo, como se trata de un ciclo, este no tiene final, ya que después de actuar, se vuelve a la planificación, luego al hacer y así sucesivamente, repitiendo todas las etapas una y otra vez durante toda la vida del sistema.

1. **Activo:**
   * Hard: Equipo (routers, switches).
   * Soft: Sistemas Operativos (Ubuntu 20.04 / Windows 10).
   * Físico: Datacenter.
   * Intangible: Conocimiento.
   * Tangible: Red de agua.
2. Los activos son los recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos.

Un activo puede no valer nada, pero si no vale nada, se puede prescindir de él porque no es necesario para que la organización funcione correctamente o alcance sus objetivos.

1. Se le denomina impacto a un activo a la medida del daño sobre el activo derivado de la materialización de una amenaza.
2. El riesgo crece con el impacto que tiene una amenaza sobre los activos y con la frecuencia con la que se presenta.
3. Las salvaguardas son las contramedidas, son los procedimientos o mecanismos que se usan para reducir los riesgos. Las hay de prevención, de organización, de política, técnicos (programas o equipos), físicos y de limitación de degradación del sistema.
4. Para asegurar la disponibilidad, confidencialidad e integridad, entre otras cosas, es necesario gestionar al personal, se lo debe educar de forma continua. Ya que no basta con asegurar que los elementos (equipamiento, software y procedimientos ) preserven la seguridad de la información, sino que también deben hacerlo los recursos humanos que utilizan dichos elementos.
5. El Dominio 8 de la ISO 27001 y 27002 trata de proteger la información de la organización antes de darle acceso a la misma a una persona, ya sea un empleado o un tercero. Esta protección debe durar lo mismo que la duración del contrato y debe persistir luego de su finalización. Busca evitar que una persona le dé un uso inadecuado a la información de la cual tiene acceso.

El dominio 8 de la ISO 27001 se refiere a la seguridad de los recursos humanos, mientras que la ISO 27002 se refiere a la protección de la información de la organización.

1. Con la ISO-IEC 71 se proponen una serie de orientaciones/recomendaciones sobre accesibilidad, centrados en los sistemas utilizados por las personas. Estas ayudan a los desarrolladores en el proceso de desarrollo de normas y estándares de accesibilidad.
2. **Clases de Controles Internos:**
   * Documentación de los Procedimientos:

Documentar y mantener actualizados los procedimientos operativos.

* + Cambios en las operaciones:

Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones.

* + Planificación de la capacidad:

Monitoreo de necesidades de capacidad de los sistemas en operación y proyección de futuras demandas, para garantizar un procesamiento y almacenamiento adecuados.

* + Protección contra el malware:

Proteger la integridad del software y la integración. Tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados.

* + Resguardo de la información:

Determinar los requerimientos para resguardar cada software o dato en función de su criticidad. Se definirá y documentará un esquema de resguardo de la información.

* + Registro de eventos:

Se producirán y mantendrán registros de auditoría en los cuales se registren las actividades, excepciones, y eventos de seguridad de la información de los usuarios, por un período acordado para permitir la detección e investigación de incidentes.

* + Software operacional:

Se debe controlar el acceso a los archivos del sistema y el código fuente del programa, y los proyectos TI. Asimismo, las actividades de soporte se debieran realizar de una manera segura. Se garantiza la seguridad de los archivos del sistema.

1. La gestión de los activos, propone tener un conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos, clasificándolos de acuerdo a la sensibilidad y criticidad de la información que contienen, para garantizar que reciban un nivel apropiado de protección y medidas de tratamiento, el cual se define a partir de su clasificación.
2. La gestión integral de seguridad incluye los temas:
   * Gestión de Activos de Información.
   * Gestión de Riesgos de Seguridad de la Información.
   * Gestión de Incidentes de Seguridad de la Información.
   * Gestión del Cumplimiento.
   * Gestión de la Continuidad del Negocio.
   * Gestión del Cambio y Cultura para la seguridad.
   * Gestión de la Estrategia de seguridad de la información.
3. Cada ACTIVO tiene 3 propiedades:
   * Confidencialidad.
   * Integridad.
   * Disponibilidad.
4. La gestión de la seguridad de la información requiere de una estrategia alineada con el negocio y sus objetivos, requiere recursos y actividades dirigidas y coordinadas por una organización de la seguridad que se extienda a través de toda la organización, desde la alta dirección hasta los usuarios finales.

Así mismo, el propietario de la información es un cargo que tiene la responsabilidad de definir quiénes tienen acceso, que pueden hacer con la información, y cuales son los requisitos para que la misma se salvaguarde ante accesos no autorizados, modificación, pérdida de confidencialidad o destrucción deliberada y qué se hace con la información una vez que ya no sea requerida.

El custodio técnico es el encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido.

El usuario es Cualquier persona que genere, obtenga, transforme, conserve o utilice información de la organización. Utilizan la información para su labor, y tendrán el derecho manifiesto de su uso dentro del inventario de información.