



GUÍA

de estudio para
Presentar ETS de la
UNIDAD DE APRENDIZAJE
Sistemas de información
seguros
Semestre 2022-2023 "B"

TURNO

Vespertino

Fecha de elaboración: 20-Abril-2023

Presidente de Academia: Carlos Francisco Arteaga Rodríguez



FORMATO DE LA GUÍA DE ESTUDIO

Área: Tecnológica	Nombre de la Unidad de Aprendizaje: Sistemas de información seguros	Nivel/semestre: Sexto
-----------------------------	---	---------------------------------

Instrucciones generales de la guía:

Anotar aspectos que el alumno debe considerar antes de presentar el examen:

ESTA GUÍA: NO TENDRÁ VALOR SOBRE LA CALIFICACIÓN FINAL DEL EXAMEN

Aquí se plasmará las características del trabajo que se debe entregar el día del ETS, donde se debe hacer una presentación sobre el caso que se plasme en el trabajo que se entrega (En forma Digital USB)

Procedimiento para la revisión del ETS.

La revisión de examen aplica solamente cuando la calificación sea de mínimo 5.

El alumno deberá asistir al área tecnológica para solicitar el formato de revisión de examen, en dónde el jefe de área firmará e informará al profesor correspondiente para realizar dicha revisión.

Ya publicada la calificación se tiene el periodo que marca la normatividad para solicitar la misma.

Presentación:

La presente guía de estudios tiene la finalidad de facilitar y proporcionar actividades correspondientes a la unidad de aprendizaje Sistemas de información seguros.

Propósito

Apoyar el estudio para adquirir los conocimientos relacionados con la unidad de aprendizaje Sistemas de información seguros

Justificación

La importancia de esta guía esta fundamentada en como la resuelva cada alumno para brindarle el desarrollo de habilidades y aprendizajes que se pretende de manera general.



Estructura y contenidos:

UNIDAD 1

- Identifica cómo es un Sistema de información.
- Reconoce los componentes y el entorno de un Sistema de Información.
- Describe los fundamentos elementales de la dirección de proyectos: Ciclo de vida, planificación, constitución y alcance.
- Analiza los riesgos y amenazas de seguridad informática de diversas organizaciones para proponer el desarrollo de un proyecto de ciberseguridad.
- Revisa las políticas internas de una organización en materia de seguridad informática.
- Evalúa la necesidad de un rediseño de la arquitectura general de un sistema de información.
- Aplica herramientas para realizar pruebas de penetración que permitan evaluar las vulnerabilidades de un sistema de información.
- Piensa crítica y reflexivamente al analizar los riesgos y amenazas a la seguridad en un Sistema de Información.
- Trabaja en forma colaborativa en la evaluación de la arquitectura general de un sistema de información.
- Desarrolla habilidades digitales y de integración de tecnologías al aplicar herramientas para evaluar la vulnerabilidad de un sistema
- Distingue los informes de ciberseguridad en base a los hallazgos que resultan de los análisis de riesgos y amenazas.
- Define los productos a entregar en un proyecto de ciberseguridad, considerando entradas, salidas y herramientas necesarias.
- Redacta los informes de ciberseguridad en base a los hallazgos que resultan de los análisis de riesgos y amenazas.
- Desarrolla el acta de constitución de un proyecto y el enunciado de su alcance.
- Establece la estrategia de ciberseguridad a seguir a partir de los análisis realizados.
- Desarrolla un cronograma con la secuencia de actividades del Proyecto de ciberseguridad a realizar.
- Realiza la estimación del costo o valor de un proyecto de ciberseguridad.
- Evalúa la factibilidad de la realización de un proyecto de ciberseguridad en una organización.

UNIDAD 2

- Distingue los sistemas de identificación, autenticación y control de acceso.
- Conoce la normatividad vigente en materia de seguridad informática.
- Organiza la documentación de los procesos de análisis, planeación, diseño, implementación y pruebas del desarrollo del proyecto de ciberseguridad basado en normas vigentes de seguridad informática.
- Establece políticas para la conformación de contraseñas y cuentas de usuario.
- Establece políticas generales de seguridad informática
- Conoce la normatividad vigente que se relaciona con aspectos de seguridad en la gobernanza de Tecnologías de Información.
- Conoce los elementos de la seguridad de la red contra ataques en tiempo real.
- Analiza si los sistemas de identificación, autenticación y control de acceso satisfagan distintos protocolos de la normatividad vigente.
- Realiza mantenimiento de datos mediante algoritmos de encriptación, creación de respaldos y eliminación permanente.
- Verifica que el acceso a bases de datos cumpla la normatividad vigente y que se satisfagan los modelos de seguridad de la información.



- Evalúa el desempeño del sistema de información seguro a partir de prototipos, simulaciones, pruebas de penetración y demostraciones en distintos escenarios.
- Realiza modificaciones al sistema de información hasta satisfacer la normatividad correspondiente, así como en aquellos casos cuya evaluación de desempeño en las pruebas realizadas aún no sean satisfactorias con los modelos de seguridad de la información.

UNIDAD 3

- Conoce la normatividad vigente relacionada con la auditoría de seguridad informática.
- Organiza la información que documenta protocolos para identificar y prevenir problemas de seguridad informática.
- Documenta el plan de acción a seguir en violaciones de políticas de seguridad informática y planes de contingencia relacionados.
- Reúne los procedimientos a seguir para reportar y recuperarse de incidentes de seguridad informática.
- Documenta los resultados obtenidos con el fortalecimiento del sistema de seguridad.
- Emite observaciones y recomendaciones como resultado de la verificación del cumplimiento de la norma de auditoría de la seguridad informática vigente.
- Conoce la normatividad vigente relacionada con la auditoría de seguridad informática.
- Revisa de manera interna que se atiendan las observaciones emitidas como resultado de la verificación del cumplimiento de las normas de auditoría de seguridad informática vigentes.
- Integra la documentación del Proyecto de Ciberseguridad.



Realizar un trabajo relacionado con Ciberseguridad en algún sistema de información que contenga mínimo lo siguiente:

1. Portada
2. índice
3. Introducción
4. Marco de trabajo
5. Estudio de Factibilidad
6. Objetivos
7. Estimación económica justificada y respaldada
8. Normatividad aplicable a su proyecto
9. Caso practico
10. Conclusiones

Se debe preparar una exposición para exponer el trabajo incluido el caso práctico el día del examen



Evaluación

La guía no tiene ningún valor para efectos del examen, lo que se va a Evaluar es el trabajo que debe entregar

Materiales para la elaboración de la guía

Ninguno en especial.

Actividades de estudio

Realizar el trabajo y preparar exposición que realizará el día del examen donde exponga lo investigado y realizar la muestra del caso práctico

Información Adicional

Además de los temas de la guía se debe estudiar todo lo relacionado a Normatividad vigente aplicable a su proyecto

Bibliografía Básica

- Guía del PMBOK - Guía de los fundamentos para la dirección de Proyecto. Séptima edición. PMI
- Solomongo CEH. (2022). ANÁLISIS DE VULNERABILIDADES: Riesgos y Amenazas. España: Solomongo.
- Brotherston, L., & Berlin, A. (2017). Defensive Security Handbook: Best Practices for Securing Infrastructure. O'Reilly Media.
- Pérez, J. C. M. (2015). Protección de datos y seguridad de la información (4a ed.). Editorial Ra-Ma.
- Dunkerley, M., & Tumbarello, M. (2020). Mastering Windows Security and Hardening: Secure and protect your Windows environment from intruders, malware attacks, and other cyber threats (English Edition) (1.a ed.). Packt Publishing.
- Vieites, G. A. (2022). Auditoría de seguridad informática. Madrid España RA-MA S.A. Editorial y Publicaciones Starbook.
- Cualquier libro actualizado relacionado con Sistemas de Información donde encuentres los temas listados en la presente Guía

INTEGRANTES DE LA ACADEMIA

Carlos Francisco Arteaga Rodríguez