



UNIVERSIDAD AUTÓNOMA DE CHIRIQUÍ  
VICERRECTORÍA ACADÉMICA  
FACULTAD DE ECONOMÍA  
ESCUELA CIENCIAS COMPUTACIONALES  
**PLANIFICACIÓN DIDÁCTICA**

Nombre de la asignatura			Abreviatura	Número	Código	Año	Semestre
<b>SEGURIDAD INFORMÁTICA</b>			PROG	431	23674	2024	II
Nombre del docente			Correo Electrónico				
Andrés Miranda Cerceño			<u>andres.miranda@unachi.ac.pa</u>				
Días en que se imparte la asignatura	Jornada	Horario	Sesiones/Horas	Horas Teóricas	Horas Prácticas	Horas de Laboratorio	Créditos
LUNES Y JUEVES	MATUTINA	7:00 – 7:45 a.m. 7:00 – 9:25 a.m.	32/64	16		48	2
Fecha de inicio de la asignatura			Fecha de culminación de la asignatura				
19 de agosto de 2024			7 de diciembre de 2024				
Fecha de revisión por el Director(a) del Departamento			Firma		Fecha de entrega al estudiante		
					19 de agosto de 2024.		
Compromisos del Estudiante							
<p><b><u>Compromiso del estudiante:</u></b></p> <ul style="list-style-type: none"> <li>✓ Asistencia puntual a las clases.</li> <li>✓ Vestuario adecuado</li> <li>✓ Uso moderado del celular.</li> <li>✓ Trabajar en equipo</li> <li>✓ Respeto a la propiedad intelectual.</li> <li>✓ Practicar las Reglas de Respeto a sus Compañeros.</li> <li>✓ Actitud para autoformarse.</li> <li>✓ Puntualidad en la entrega de actividades asignadas</li> </ul> <p><b><u>Todos los Trabajos y/o Asignaciones deben ser Sustentadas en la Fecha de Entrega.</u></b></p>							

EJE TEMÁTICO	N° 1	<b>CONCEPTOS BÁSICOS DE SEGURIDAD INFORMÁTICA</b>	
<b>COMPETENCIAS GENÉRICAS</b>		Investiga conceptos, características y Técnicas para la Seguridad Informática	
<b>COMPETENCIAS ESPECÍFICAS</b>		Comprende y asocia los conceptos de seguridad física y lógica en la informática. Identifica y evalúa riesgos y vulnerabilidades para implementar normas y políticas de seguridad.	
FECHA	CONTENIDOS	<b>ACTIVIDADES ACADÉMICAS INNOVADORAS APLICADA POR EL DOCENTE</b>	
19-agosto 20-septiembre	I. Seguridad Informática 1.1 Introducción 1.2 Conceptos de seguridad informática. 1.3 Objetivos de la Seguridad 1.3.1 Integridad 1.3.2 Disponibilidad 1.3.3 Confidencialidad 1.4 Algunas afirmaciones erróneas comunes acerca de la seguridad 1.5 Tipos de Recursos 1.6 Amenazas a la Seguridad de la Información 1.6.1 Personas 1.6.2 Amenazas lógicas 1.6.2.1 Software Incorrecto 1.6.2.2 Herramientas de Seguridad 1.6.2.3 Puertas Traseras 1.6.2.4 Virus 1.6.2.5 Gusanos 1.6.2.6 Otros 1.7 Catástrofe	✓ Investiga y Sustenta sobre los conceptos y características de la Seguridad Informática.  ✓ Desarrolla diversos laboratorios con los temas relacionados a la Seguridad Informática  ✓ Interactúa de forma grupal, para el desarrollo de talleres en clases, sobre casos de estudios.  ✓ Investiga herramientas para la evitar riesgos en la Seguridad Informática  ✓ Presenta prueba parcial escrita.	
ESTRATEGIAS DE APRENDIZAJE (las que utilizará el estudiante)		ACTIVIDADES ACADÉMICAS	
		DE INVESTIGACIÓN	DE EXTENSIÓN
✓ Investigaciones, Casos de Estudios o Talleres, Trabajos Grupales, Proyectos,		Investiga los Conceptos y Características de la Seguridad Informática	

	Investiga Herramientas para evitar riesgos en la Seguridad Informática.	
TECNICA O ESTRATEGIA DE EVALUACIÓN	RECURSOS Y TECNOLOGÍA APLICADA EN EL PROCESO DE ENSEÑANZA Y APRENDIZAJE	
Investigación, Análisis, Proyecto Sustentado, Prueba Parcial.	Computadora con Software de Aplicación, Material Fotocopiado, Data Show, Bibliografía Digital, Software de Aplicación para Documentación de Manual de Usuario, Plataforma Virtual.	
FUENTES BIBLIOGRÁFICAS		
<ul style="list-style-type: none"><li>✓ McClure, Stuard. Hackers: Secreto y soluciones para la seguridad de redes.2000</li><li>✓ Fitzgerald, Jerry. Comunicación de datos en los negocios: conceptos básicos, seguridad y diseño / Fitzgerald, Jerry, edición 1. México, D.F. : Megabyte , 1993.</li><li>✓ McCarthy, Mary Patt. Seguridad digital: estrategias de defensa digital para proteger la reputación y la cuota de mercado de su compañía / McCarthy, Mary Patt, edición 1</li><li>✓ Norton Peter. “Introducción a la Computación”. México. 2006.</li></ul>		

EJE TEMÁTICO	Nº 2	ANÁLISIS Y ESTUDIO DE POLÍTICAS DE SEGURIDAD	
COMPETENCIAS GENÉRICAS		Evalúa y Analiza Políticas de Seguridad Física y Lógica	
COMPETENCIAS ESPECÍFICAS		Capacidad de abstracción, análisis y síntesis. Capacidad de aplicar los conocimientos en la práctica. Capacidad de organizar y planificar el tiempo.	
FECHA	CONTENIDOS		ACTIVIDADES ACADÉMICAS INNOVADORAS APLICADA POR EL DOCENTE
23 septiembre – 25 octubre	<div>II. SEGURIDAD FÍSICA</div> <div>2.1 Historia</div> <div>2.2 Funcionamiento y rendimiento</div> <div>2.3 Tabla comparativa de sistemas biométricos</div> <div>2.4 Estándares asociados a tecnologías biométricas.</div> <div>2.5 Procesos de Autenticación e Identificación biométrica</div> <div>III. SEGURIDAD LÓGICA</div> <div>3.1 Daños y perjuicios</div> <div>3.2 Métodos de contagio</div> <div>3.3 Seguridad métodos de protección</div> <div>3.4 Filtros de ficheros</div> <div>3.5 Estrategias de Seguridad</div> <div>3.5.1 Identificar métodos, herramientas y técnicas de ataques</div> <div>3.5.2 Establecer estrategias Proactivas y Reactivas</div> <div>3.6 Planificación</div> <div>3.7 Consideraciones de software</div> <div>3.8 Consideraciones de la red</div> <div>3.8.1 Política general</div> <div>3.8.2 Formación: Del usuario</div> <div>3.8.3 Antivirus</div> <div>3.8.4 Firewall</div>		<div>✓ Investiga y Sustenta sobre los Conceptos y Características de Seguridad Física y Lógica</div> <div>✓ Analiza herramientas de seguridad y aplicación de software</div> <div>✓ Evalúa y Analiza Políticas de Seguridad</div> <div>✓ Analiza Estrategias de Seguridad</div> <div>✓ Presenta Prueba Parcial Escrita.</div>
ESTRATEGIAS DE APRENDIZAJE (las que utilizará el estudiante)			ACTIVIDADES ACADÉMICAS

	DE INVESTIGACIÓN	DE EXTENSIÓN
✓ Investigaciones, Proyectos, Prueba Parcial.	Analiza y Evalúa políticas de Seguridad Analiza herramientas de seguridad Analiza estrategias de seguridad	
TECNICA O ESTRATEGIA DE EVALUACIÓN	RECURSOS Y TECNOLOGÍA APLICADA EN EL PROCESO DE ENSEÑANZA Y APRENDIZAJE	
Investigación, Análisis de Herramientas, Políticas de Seguridad, Proyecto Sustentado, Prueba Parcial.	Computadora con Software de Aplicación, formulario de encuestas, Software de Aplicación Gráfico, Data Show, Bibliografía Digital, Software de Aplicación para Documentación de Manual de Usuario, Plataforma Virtual.	
FUENTES BIBLIOGRÁFICAS		
✓ Mcclure, Stuard. Hackers: Secreto y soluciones para la seguridad de redes.2000 ✓ Fitzgerald, Jerry. Comunicación de datos en los negocios: conceptos básicos, seguridad y diseño / Fitzgerald, Jerry, edición 1. México, D.F. : Megabyte , 1993. ✓ McCarthy, Mary Patt. Seguridad digital: estrategias de defensa digital para proteger la reputación y la cuota de mercado de su compañía / McCarthy, Mary Patt, edición 1 ✓ Norton Peter. “Introducción a la Computación”. México. 2006.		

<b>EJE TEMÁTICO</b>	<b>N° 3</b>	<b>PLANEACIÓN DE SEGURIDAD EN RED, AUDITORÍA DE SISTEMAS Y OTROS</b>	
<b>COMPETENCIAS GENÉRICAS</b>		Análisis y Evaluación de Políticas de Seguridad en Red y Auditoria de Sistemas.	
<b>COMPETENCIAS ESPECÍFICAS</b>		Capacidad de abstracción, análisis y síntesis. Capacidad de aplicar los conocimientos en la práctica. Capacidad de organizar y planificar el tiempo.	
<b>FECHA</b>	<b>CONTENIDOS</b>		<b>ACTIVIDADES ACADÉMICAS INNOVADORAS APLICADA POR EL DOCENTE</b>
28 octubre - 6 diciembre	IV. Planeación de Seguridad en Red 4.1 Políticas de Seguridad en el sitio 4.2 Análisis de Riesgos 4.3 Identificación de Recursos 4.4 Identificación de Amenazas 4.5 Definir accesos de Información 4.6 ¿Cómo diseñar una Política de Red? V. Auditoria de Sistemas 5.1 ¿Qué es una Auditoria de Sistemas? 5.2 Evaluación de: 5.2.1 Sistemas 5.2.2 Análisis 5.2.3 Diseño Lógico del Sistema 5.2.4 Desarrollo del Sistema 5.3 Control de Proyectos VI. Seguridad en Centros de Cómputo 6.1 Recursos de T.I. 6.2 Dominios 6.3 Gestión de Tecnologías 6.3.1 COBIT 6.3.2 CISA 6.3.3 ISACA 6.3.4 Otros		✓ Investiga y Sustenta sobre las Políticas de Seguridad en Red ✓ Análisis sobre los Riesgos que se encuentran dentro de la Seguridad Informática ✓ Investiga sobre las estrategias para la Auditoria de Sistemas ✓ Evaluación de la Seguridad dentro de los Centros de Cómputo ✓ Desarrolla y Sustenta Proyecto con Herramientas de Seguridad
<b>ESTRATEGIAS DE APRENDIZAJE (las que utilizará el estudiante)</b>		<b>ACTIVIDADES ACADÉMICAS</b>	
		<b>DE INVESTIGACIÓN</b>	<b>DE EXTENSIÓN</b>

✓ Investigaciones, Laboratorios, Proyecto.	Investiga y Sustenta sobre las Políticas de Seguridad en Red Investiga y sustenta sobre Auditoria de Sistemas Presenta Políticas dentro de un Centro de Cómputo	
TECNICA O ESTRATEGIA DE EVALUACIÓN	RECURSOS Y TECNOLOGÍA APLICADA EN EL PROCESO DE ENSEÑANZA Y APRENDIZAJE	
Investigación, Proyecto Sustentado.	Computadora con Software de Aplicación, formulario de encuestas, Software de Aplicación Gráfico, Data Show, Bibliografía Digital, Software de Aplicación para Documentación de Manual de Usuario, Plataforma Virtual.	
FUENTES BIBLIOGRÁFICAS		
<ul style="list-style-type: none"><li>✓ McClure, Stuard. Hackers: Secreto y soluciones para la seguridad de redes.2000</li><li>✓ Fitzgerald, Jerry. Comunicación de datos en los negocios: conceptos básicos, seguridad y diseño / Fitzgerald, Jerry, edición 1. México, D.F. : Megabyte , 1993.</li><li>✓ McCarthy, Mary Patt. Seguridad digital: estrategias de defensa digital para proteger la reputación y la cuota de mercado de su compañía / McCarthy, Mary Patt, edición 1</li><li>✓ Norton Peter. “Introducción a la Computación”. México. 2006.</li></ul>		

# Universidad Autónoma de Chiriquí

## Facultad de Economía

### Licenciatura en Gestión de Tecnología de Información

Asignatura: Seguridad Informática

**PROG 431**

Profesor: Andrés Miranda C.

Cód. de Asig.: 23674

Fecha: 19-agosto-2024

#### Evaluación Semestral

Dos (2) Parciales	30%
Proyectos, Laboratorios, Investigaciones, Tareas, Talleres	35%
Examen Semestral - Desarrollo de Aplicación	35%
<b>Total de la Evaluación</b>	<b>100%</b>

### Cronograma de Actividades

Fecha	Tipo de Actividad	Contenido	Valor (%)	Evaluación
Jueves 26 de Septiembre	Parcial No. 1	Eje Temático No. 1 Conceptos Básicos de Seguridad Informática	15	Presencial (Teórico/Práctico)
Jueves 7 de Noviembre	Parcial No. 2	Eje Temático No. 2 Análisis y Estudio de Políticas de Seguridad	15	Presencial (Teórico - Práctico)
		<b>PROYECTOS</b>		
Jueves 19 de Septiembre	Proyecto No.1	Conceptos Básicos de Seguridad Informática y Herramientas	8	Presencial - Investigación y Sustentación
Jueves 31 de Octubre	Proyecto No.2	<b>Evaluación de Herramientas y Seminario de Emprendimiento</b>	8	Presencial - Investigación y Sustentación
Jueves 21 de Noviembre (Uso y Aplicación de software * Manual de Usuarios*)	<b>Proyecto No. 3</b>	<b>** Portafolio Tecnológico **</b> Incluye todos los lab., Proy. Parc., Inv., tareas, entre otros.	10	Presencial (Lab. Práctico) y Sustentación
Laboratorios	Lab.	<b>Laboratorios Prácticos</b> (Software para Complemento de las clases teóricas)	5	Presencial (Lab. Práctico y Sustentación)
Investigaciones	Inv.	Investigación de conceptos de Ingeniería de software	2	Presencial y Sustentación
Estudio de Casos	Casos	Desarrollar casos de estudios	2	Presencial y Sustentación
		Total de Proy. Inv. Lab.	<b>35%</b>	

**IMPORTANTE:** TODOS LOS TRABAJOS Y ASIGNACIONES, DEBERÁN SER SUSTENTADAS POR EL ESTUDIANTE, DE LO CONTRARIO **NO TENDRÁN DERECHO A SU VALOR ASIGNADO.**

**¡SEGUIMOS AVANZANDO...CON LA AYUDA DE DIOS!**



# Seguridad Informática



**UNACHI – FAC- DE ECONOMÍA – LIC. GESTIÓN DE T. I.**

***Prof. Andrés Miranda Cerceño***

**Septiembre de 2024**

# ¿Qué es la Seguridad Informática?

La Seguridad Informática es una especialidad o disciplina con la disponibilidad de proteger la estructura de los computadores y todos los dispositivos electrónicos.

Dentro de la Protección de la Seguridad Informática, podemos destacar algunos conceptos, tales como:

- ✓ Salvaguardar la confidencialidad de los datos.
- ✓ Preservar la integridad de los datos.
- ✓ Generar la disponibilidad de datos para usuarios autorizados.
- ✓ Proteger la autenticidad de la información.

# Objetivos de la Seguridad Informática

## Confidencialidad:

Los ciberdelincuentes cada día utilizan métodos y herramientas que son una amenaza para la información de las empresas Privadas o Públicas. Todo profesional del área de Tecnología, que tiene a su cargo la creación, implementación o de mantener la estructura de seguridad informática, debe tener claro lo importante que TODO es Confidencial.

## Integridad:

Todo profesional en el área de Tecnología de ciberseguridad o Seguridad Informática es necesario asegurar que bajo ninguna circunstancia se pueden modificar los datos . Es Importante tener claro que los datos tengan una seguridad, que estén protegidos de un borrado, además de otras prácticas como las copias de seguridad.



## Disponibilidad:

Solo los usuarios o las personas que tengan la autorización, pueden acceder a los sistemas, los datos o informaciones, en el momento que se necesiten o se soliciten.

## **Organismos de Normalización Internacionales**

Las siglas ISO/IEC se refieren a los organismos de normalización internacionales. ISO es la Organización Internacional de Normalización, y IEC es la Comisión Electrotécnica Internacional. Estos organismos establecen estándares y certifican empresas que cumplen con altos estándares de calidad en sus procesos

**ISO/IEC 27002** proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

# ¿Qué es Zero Trust?

Forrester creó este concepto en 2010 en contraste con el modelo de seguridad tradicional que se basa en la premisa de "**confiar pero verificar**".

Zero Trust, en cambio, establece que las organizaciones nunca deben confiar en una entidad ya sea interna o externa. En otras palabras, "**nunca confíes, verifica siempre**".

El modelo Zero Trust crea seguridad en torno a cada uno de los recursos y entidades clave de una organización: datos, redes, dispositivos, cargas de trabajo y personas.

**Data**



**Networks**

**Devices**

**Workloads**



**People**



- ✓ VISIBILITY
- ✓ POLICIES
- ✓ AUTOMATION

## ¿Qué debe hacer una organización para implementar el modelo de confianza cero?

Hay tres áreas centrales de capacidad que una organización debe desarrollar a medida que implementas el **modelo Zero Trust**:

1. **Visibilidad:** identifique los dispositivos y recursos que se deben supervisar y proteger. No es posible proteger un recurso que no conoce. Tener visibilidad de todos sus recursos y puntos de acceso es indispensable.
2. **Políticas:** Establezca controles que solo permitan que personas específicas tengan acceso a recursos específicos en condiciones específicas. En otras palabras, se requiere un nivel granular de controles de directiva.
3. **Automatización:** Automatice los procesos para garantizar la correcta aplicación de las políticas y permitir que la organización se adapte rápidamente a cualquier desviación de los procedimientos estándar.

Basándose en las capacidades fundamentales descritas aquí, podemos definir Zero Trust como un modelo de seguridad que construye defensas alrededor de cada una de las siguientes entidades: **datos, redes, dispositivos, cargas de trabajo y personas.**



# ¿Cómo funciona una arquitectura de confianza cero o seguridad Zero Trust?

La **Implementación de Confianza Cero** implica requerir una verificación de identidad estricta para cada persona o dispositivo que intente acceder a la red o aplicación. Esta verificación se aplica independientemente de si el dispositivo o usuario ya está dentro del perímetro de la red.

## La Superficie de Protección

La protección comienza identificando su superficie de protección, que se basa en datos, aplicaciones, activos o servicios, comúnmente referidos por el acrónimo **DAAS**:

- ✓ **Datos:** ¿Qué datos tiene que proteger?
- ✓ **Aplicaciones:** ¿Qué aplicaciones tienen información confidencial?
- ✓ **Activos:** ¿Cuáles son sus activos más sensibles?
- ✓ **Servicios:** ¿Qué servicios puede vulnerar un actor malicioso en un intento de interrumpir el funcionamiento normal de TI?

Establecer esta superficie de protección, le ayuda a perfeccionar exactamente lo que debe protegerse.



Una política de confianza cero o modelo Zero Trust, implica regular el tráfico relacionado con los datos y componentes críticos mediante la formación de microperímetros.

En el borde de un microperímetro, una red de confianza cero emplea una **Puerta de Enlace de Segmentación**, que monitorea la entrada de personas y datos. Aplica medidas de seguridad diseñadas para examinar exhaustivamente a los usuarios y datos antes de otorgar acceso utilizando un firewall de Capa 7 y el método Kipling.

Una regla de **Capa 7** implica inspeccionar la carga útil de paquetes para ver si coinciden con los tipos de tráfico conocidos.

Si un paquete contiene datos que no cumplen con los parámetros de la regla de **Capa 7**, el acceso se bloquea.

El método de Kipling cuestiona la validez del intento de participación haciendo seis preguntas sobre la participación y quién está tratando de ingresar: **¿Quién? ¿Qué? ¿Cuándo? ¿Dónde? ¿Por qué? ¿Cómo?** Si la respuesta a cualquiera de las

## ¿Qué es un escritorio como servicio (DaaS)?

**Desktop-as-a-Service (DaaS)** es una forma de ofrecer entornos completos de escritorios virtuales a los usuarios, incluidos sistemas operativos, aplicaciones, archivos y preferencias de usuario desde la nube. Los escritorios se ejecutan en **Virtual Machines** alojadas en una infraestructura de computación, almacenamiento y red administrada por el proveedor de la nube.

Los usuarios pueden acceder a su entorno de escritorio desde una amplia variedad de dispositivos, incluidos PC, computadoras portátiles, tabletas y algunos smartphones.

Muchas organizaciones buscan una alternativa al modelo tradicional de despliegue de escritorio, en el que los administradores de TI instalan un sistema operativo y aplicaciones en cada dispositivo de los empleados.

Con ese modelo, los administradores suelen gastar demasiado tiempo y dinero instalando software, administrando actualizaciones e intentando proteger los dispositivos.

# **DaaS versus infraestructura de escritorio virtual**

Al igual que las ofertas de DaaS, las soluciones de infraestructura de escritorio virtual (VDI) ofrecen escritorios a dispositivos desde un centro de datos centralizado.

Con el modelo DaaS, la infraestructura de **cómputo, almacenamiento y red** son gestionadas por un proveedor de la nube.

La organización que proporciona escritorios a sus empleados puede administrar el **sistema operativo de escritorio, las aplicaciones, el software antivirus** y cualquier otra tarea relacionada con el escritorio, o trabajar con un proveedor de servicios de escritorio administrado por terceros.