

**Informe Diario**

**Juan Esteban Catalan Sanchez**

**Corporación Universitaria Minuto de Dios**

**​Rectoría Bogotá Región (Bogotá)​**

**Centro Universitario ​Noroccidente Bogotá (Engativá)​**

**Programa ​Ingeniería de Sistemas​**

**​​ 15 de septiembre de 2025​**

CONTENIDO

[1. Introducción 3](#_Toc209453527)

[2. Objetivos 3](#_Toc209453528)

[Objetivo general 3](#_Toc209453529)

[Objetivos específicos 3](#_Toc209453530)

[3. Metodología 3](#_Toc209453531)

[4. Desarrollo de las Clases 3](#_Toc209453532)

[Clase 1 – [11/08/2025] 3](#_Toc209453533)

[Clase 2 – [14/08/2025] 4](#_Toc209453534)

[Clase 3 – [18/08/2025] 4](#_Toc209453535)

[Clase 4 – [21/08/2025] 4](#_Toc209453536)

[Clase 5 – [25/08/2025] 5](#_Toc209453537)

[Clase 6 – [28/08/2025] 9](#_Toc209453538)

[Clase 7 – [01/09/2025] 14](#_Toc209453539)

[Clase 8 – [04/09/2025] 21](#_Toc209453540)

[Clase 9 – [08/09/2025] 24](#_Toc209453541)

[Clase 10– [11/09/2025] 28](#_Toc209453542)

[Clase 10– [11/09/2025] 35](#_Toc209453543)

[5. Conclusiones 35](#_Toc209453544)

[6. Bibliografía 36](#_Toc209453545)

# 1. Introducción

El presente informe tiene como propósito evidenciar las actividades realizadas en cada clase durante el corte académico de la asignatura. A lo largo del documento se registran los temas, actividades, aprendizajes y observaciones de cada sesión, con el fin de analizar el proceso formativo.

# 2. Objetivos

## Objetivo general

Registrar y analizar las actividades realizadas en clase durante el corte académico, enfocadas en la comprensión y aplicación de los principios de seguridad de la información.

## Objetivos específicos

* Describir las actividades y prácticas desarrolladas en cada sesión relacionadas con la protección de la información.
* Evidenciar los aprendizajes adquiridos sobre conceptos, normativas, herramientas y buenas prácticas en seguridad de la información.
* Identificar los aportes personales y grupales en el fortalecimiento de una cultura de seguridad digital.
* Reconocer la importancia de la seguridad de la información en los entornos académicos, laborales y personales.

# 3. Metodología

El informe se elaboró mediante el registro sistemático de cada clase, incluyendo los temas tratados, las actividades realizadas y las reflexiones personales sobre los aprendizajes obtenidos. La información fue recopilada a partir de apuntes de clase, materiales proporcionados por el docente y las experiencias de participación activa.

# 4. Desarrollo de las Clases

## Clase 1 – [11/08/2025]

• **Tema central**

inicialización de la materia e introducción a la Seguridad de la Información

• **Actividades realizadas**

* Esta por ser la primera clase el profesor nos dio como la metodología que iba usar para calificarnos en la materia como se estructuraba y menciono temas que se iban abordar a lo largo del corte, esto fue clave para saber que temas repasar para lo que requiere la materia

• **Aprendizajes obtenidos**

* Reconocí la importancia de la seguridad de la información como un pilar fundamental en la protección de datos personales y empresariales.
* Comprendí los riesgos más comunes que existen en el mundo digital, como el robo de identidad, fraudes electrónicos y ataques de malware

## Clase 2 – [14/08/2025]

• No se realizo clase por un compromiso personal del instructor.

## Clase 3 – [18/08/2025]

• No se realizo clase por que era día Festivo

## Clase 4 – [21/08/2025]

• **Tema central**

Escaneos y Protocolos de Red

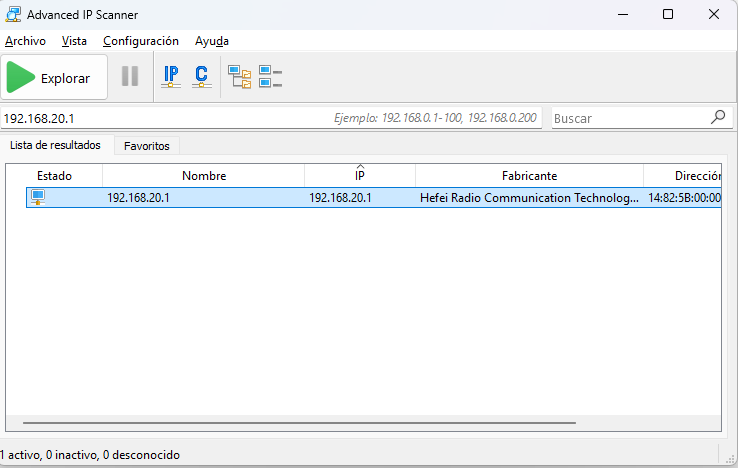
• **Actividades realizadas**

Definiciones de:

* **CIA (Confidencialidad, Integridad, Disponibilidad)**
* **Confidencialidad:** Que la información solo la vean los autorizados.
* **Integridad:** Que los datos no se cambien ni dañen sin permiso.
* **Disponibilidad:** Que la información esté accesible cuando se necesite.
* **DIC (Disponibilidad, Integridad, Confidencialidad)**

Es lo mismo que CIA, solo cambia el orden:

* **Disponibilidad primero** → que la info siempre esté lista.
* **Integridad** → que no se altere.
* **Confidencialidad** → que no cualquiera la vea.
* **SNMP (Simple Network Management Protocol):**
* Es un protocolo de red que permite la **administración y monitoreo de dispositivos conectados** como routers, switches, servidores o impresoras. A través de él se pueden obtener datos sobre el estado de los equipos, supervisar su funcionamiento y recibir alertas en caso de fallos.
* Advanced ip Scanner



• **Aprendizajes obtenidos:**

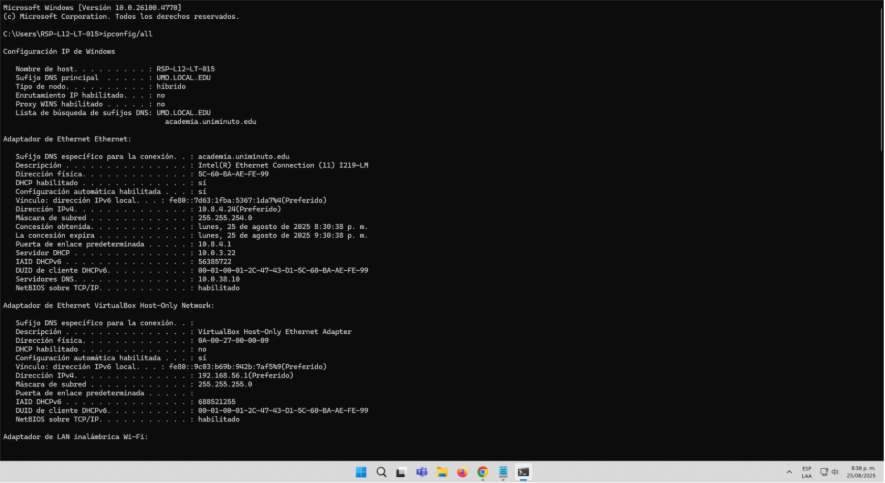
* Aprendí la importancia de los principios **CIA/DIC** en la seguridad de la información, el uso de **SNMP** para administrar dispositivos de red y la utilidad de **Advanced IP Scanner** para identificar equipos conectados.

## Clase 5 – [25/08/2025]

• Tema central  
Escaneo de puertos del localhost utilizando MobaXterm y análisis de servicios en ejecución.

• Actividades realizadas

* Se ejecutó el comando ipconfig /all para identificar la configuración de red del equipo (IP, máscara de subred, DNS, etc.)



Practica en casa   
Texto

El contenido generado por IA puede ser incorrecto.

* Se revisaron conceptos básicos como **DOM**, su estructura, y el uso de **PID** en la gestión de procesos.

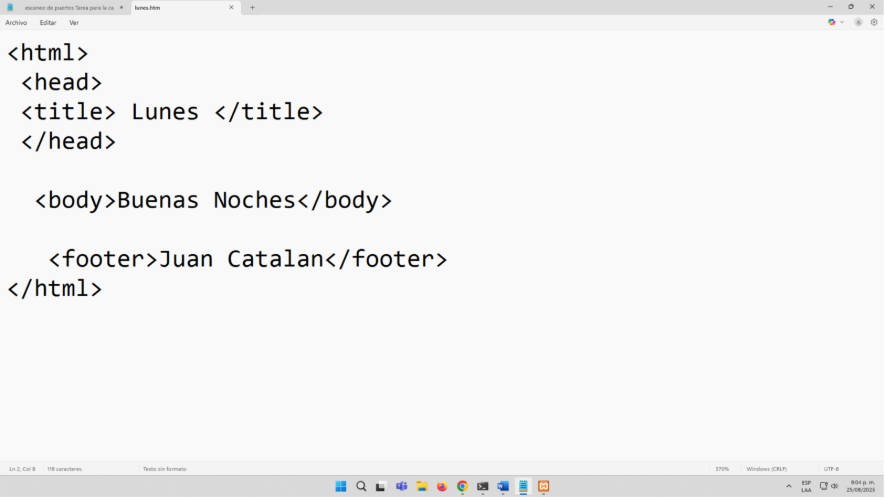
🔹 **DOM (Document Object Model):** Es la forma en que los navegadores representan un documento HTML. Se organiza como un árbol donde cada etiqueta (head, body, párrafos, imágenes, etc.) es un nodo. Gracias al DOM se pueden manipular elementos de una página con lenguajes como JavaScript.

🔹 **PID (Process Identifier):** Es un número único que el sistema operativo asigna a cada proceso en ejecución. Sirve para identificar, controlar o finalizar procesos en la computadora.

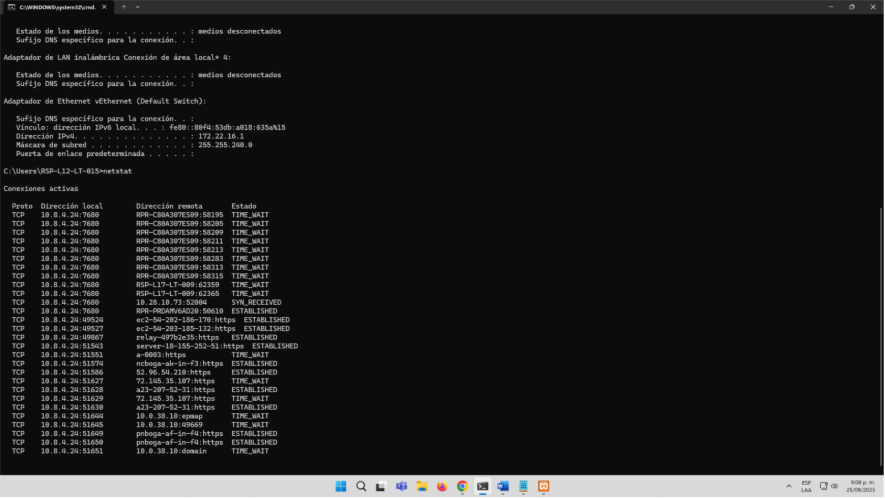
* Se creó un archivo con extensión .htm y se habilitó el servicio **Apache** para simular la publicación de contenido web.

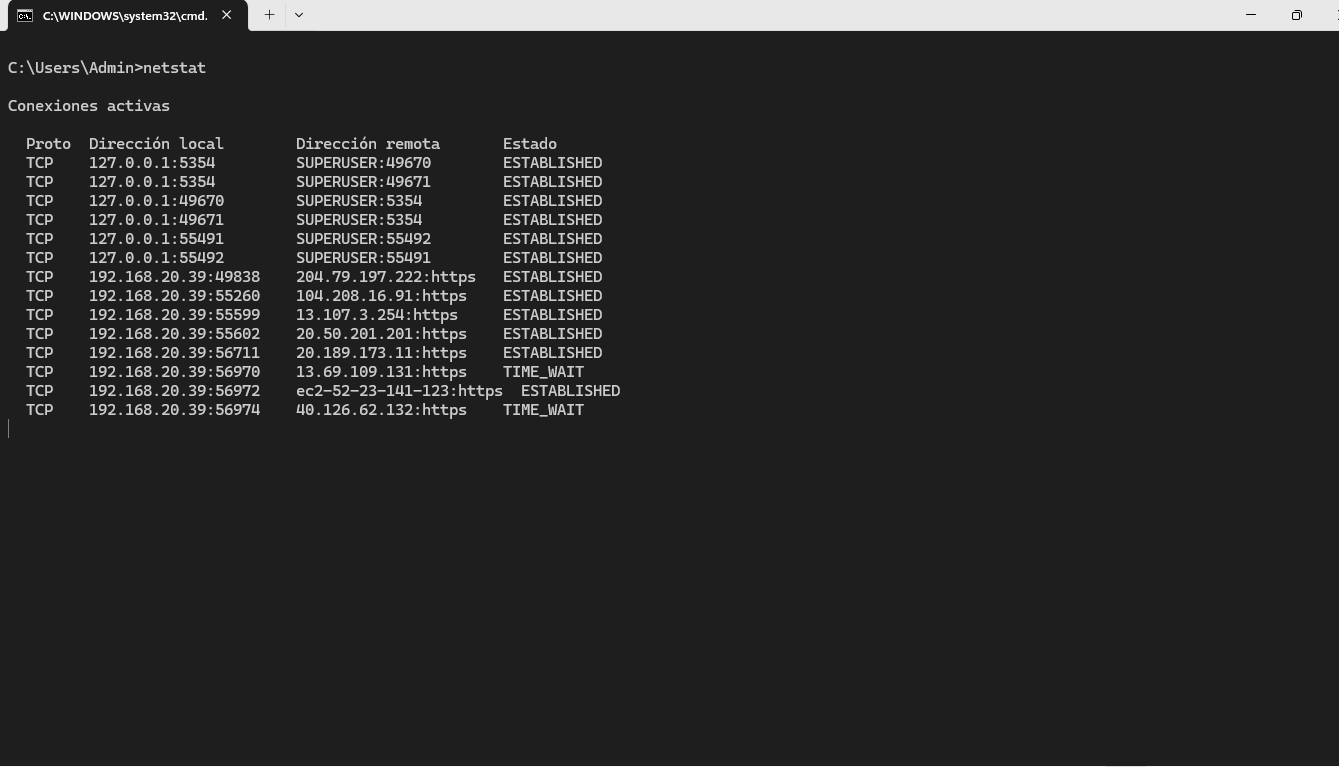
Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.



* Con el comando netstat, se analizaron las conexiones activas y procesos asociados.



Practica en casa   


* Se utilizó **MobaXterm** para realizar el escaneo de puertos en el localhost y visualizar qué servicios estaban en ejecución

• Aprendizajes obtenidos:

* Comprendí cómo identificar la configuración de red de un equipo y la importancia de cada parámetro en la conectividad.
* Aprendí el concepto de DOM y su estructura dentro de un archivo HTML.
* Reconocí el papel de los procesos y servicios en la comunicación de red, así como la relevancia del PID para gestionarlos.

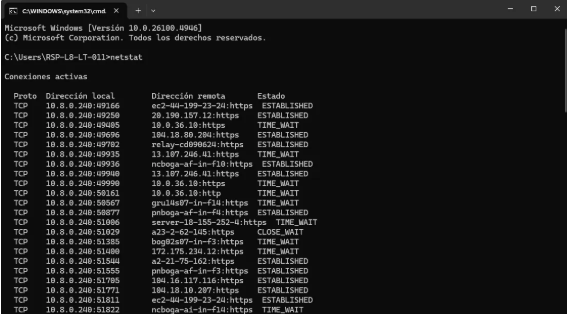
## Clase 6 – [28/08/2025]

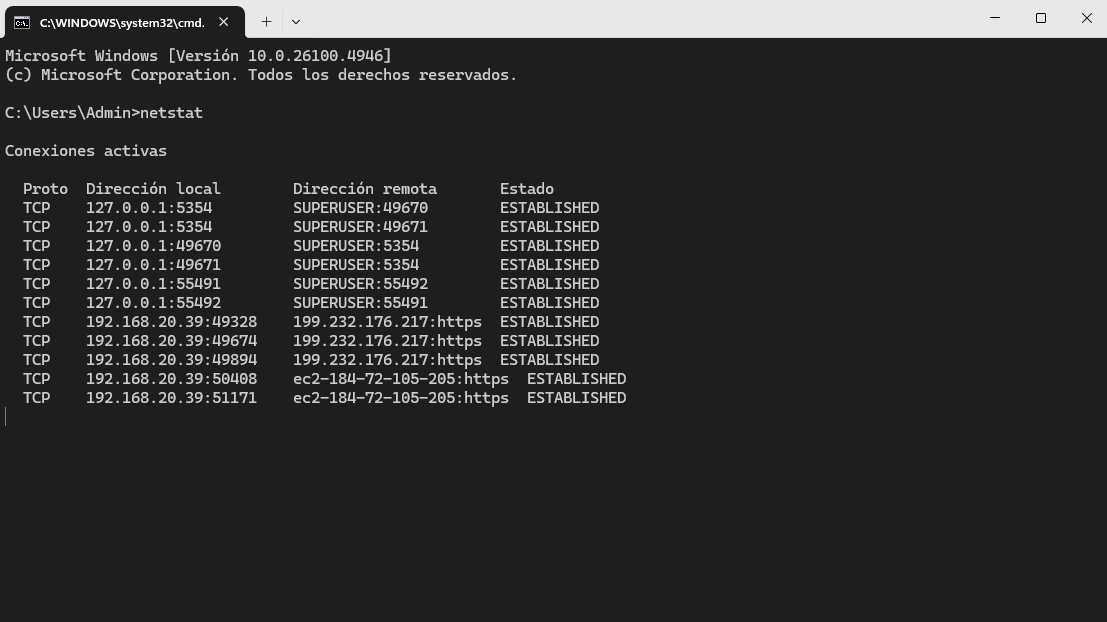
• Tema central

* **SQL Injection**

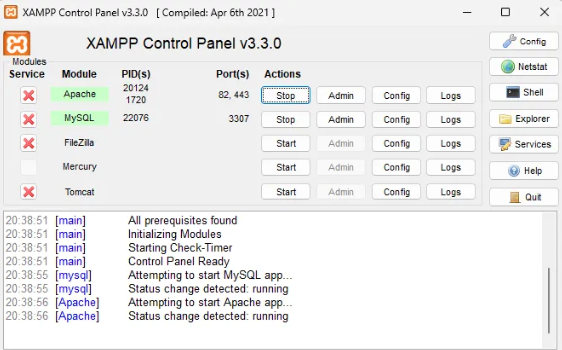
• Actividades realizadas

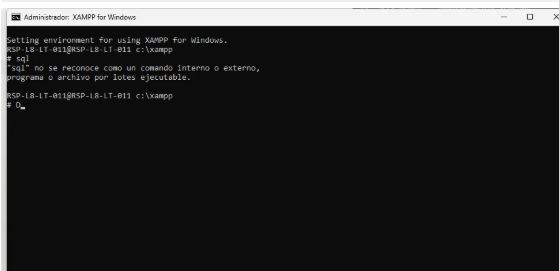
* Aplicar un netstat por cmd y verificar los puertos que estan en usos y abrir xamp



Practica en casa   


* Habilitar MySQL en Xampp



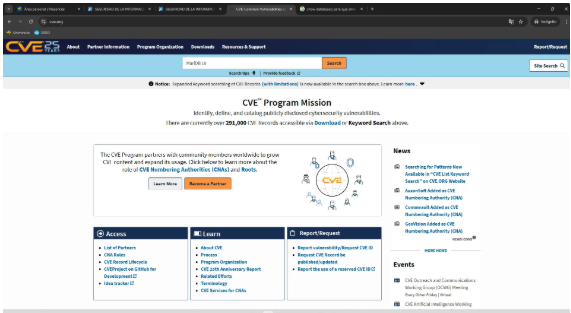


Se abre el modo administrador

Interfaz de usuario gráfica, Aplicación

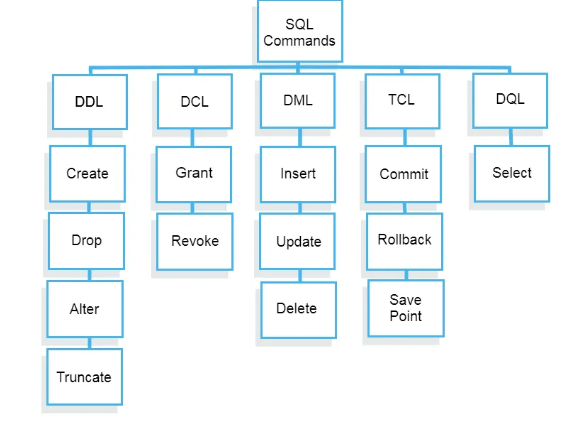
El contenido generado por IA puede ser incorrecto.

Dirigirse a [cve.org](http://cve.org/) y biscar si MariaDB 10 es vulnerable



Se aplica el siguiente comando para **mostrar una lista de todas las bases de datos disponibles en el servidor de bases de datos de MySQL o MariaDB al que estás conectado.**Texto

El contenido generado por IA puede ser incorrecto.

**Tipos de lenguajes SQL  
**

**Abrir un archivo de texto y crear una tabla   
Interfaz de usuario gráfica, Texto, Aplicación, Word

El contenido generado por IA puede ser incorrecto.**

• Aprendizajes obtenidos:

* Uso de **netstat** para identificar puertos en uso.
* Habilitación de **MySQL en XAMPP** y acceso en modo administrador.
* Consulta de vulnerabilidades en **cve.org** (ejemplo: MariaDB 10).
* Ejecución de comandos básicos en MySQL/MariaDB para listar bases de datos.
* Reconocimiento de los **tipos de lenguajes SQL** (DDL, DML, DCL, TCL).

## Clase 7 – [01/09/2025]

• Tema central

* Las herramientas/normas que permiten proteger los datos y redes frente a vulnerabilidades y ataques.

• Actividades Realizadas:

**Normas ISO**

* **ISO 27001:2013** → Una guía que ayuda a las empresas a crear un sistema de protección de la información.
* **ISO 27001:2022** → Además de proteger la información, también incluye ciberseguridad, pensando en ataques modernos (hackeos, ransomware, phishing, etc.).

**Conceptos**

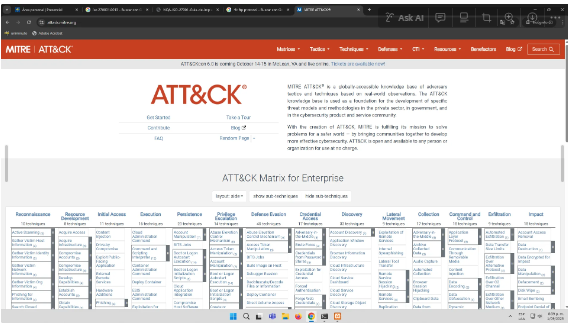
RFC → Son documentos que explican cómo funcionan las reglas de internet (como un manual de uso).

CVE → Es una lista pública donde aparecen las fallas y vulnerabilidades conocidas de sistemas y programas. (Como una “cartelera de advertencias”).

**Fases del hacking**

Un hacker (ético o no) sigue normalmente estas fases:

1. **Reconocimiento** → Buscar información del objetivo.
2. **Escaneo** → Revisar puertos, servicios y debilidades.
3. **Explotación** → Intentar entrar por esas fallas.
4. **Mantener acceso** → Si lo logra, busca quedarse dentro sin ser detectado.
5. **Borrar huellas** → Ocultar lo que hizo.

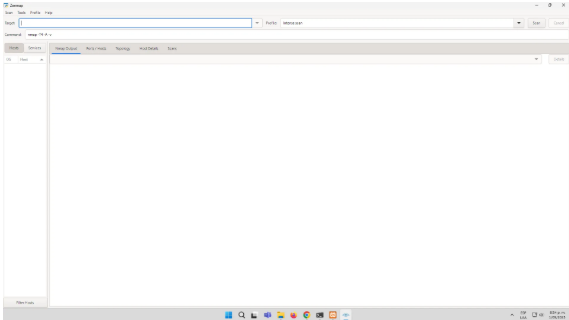
En esta pagina es una buena herramienta para entender todo el tipo de hackeos y encuentra de vulnerabilidades  
  
**Protocolos y herramientas**

* **FTP** → Sirve para **subir y bajar archivos entre dos computadoras** (ejemplo: de tu PC a un servidor).
* **SSH / SFTP (Puerto 22)** → Forma segura de conectarse a otro equipo a distancia. Es como usar FTP, pero con seguridad extra.
* **Nmap** → Herramienta para **escaneo de redes**: sirve para descubrir qué equipos están conectados y qué puertos o servicios tienen abiertos.  
  **INSTALACION**

Interfaz de usuario gráfica, Texto, Aplicación

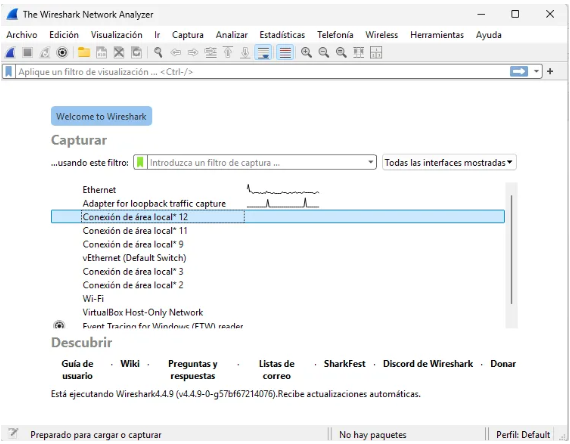
El contenido generado por IA puede ser incorrecto.  
Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

Entrar a NMAP  
  
Escanear al [localhost](http://localhost/) o en este caso la ip del profesor

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.  
IMPORTANTE → Es necesario identificar para que es el escaneo si es para ipv4, ipv6, DNS o localhost

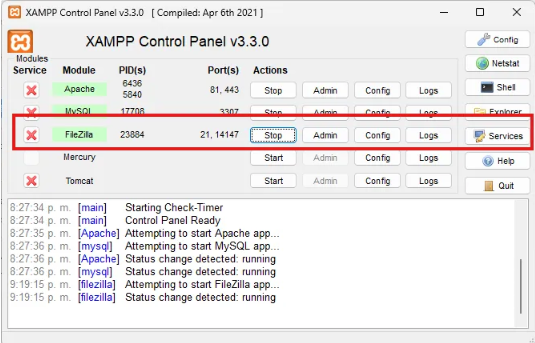
* **Wireshark** → Captura el tráfico de red (como una grabadora que escucha todo lo que pasa entre las computadoras).  
  

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.  
Seleccionamos un paquete cualquiera y se le hace un breve escaneo de la información que nos imprime  
Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.  
Ese paquete en **Wireshark** es un mensaje de **descubrimiento de red (EDP)**.  
El dispositivo con dirección **MAC 00:0c:29:8c:c1:42** está diciendo:  
*“Estoy conectado a la red, aquí están mis datos básico”*

* **FileZilla** → Programa sencillo para **usar FTP/SFTP** y mover archivos.

Se Activo el servicio  


* **OWASP** → Comunidad que publica el **Top 10 de vulnerabilidades más comunes en aplicaciones web**.
* **Meta Data** → Información escondida dentro de un archivo (ejemplo: un Word puede tener autor, fecha de creación, etc.).
* Aprendizajes Obtenidos
  + Las normas **ISO 27001** guían a las empresas en buenas prácticas de seguridad.
  + **RFC y CVE** ayudan a entender reglas de internet y vulnerabilidades conocidas.
  + Las **fases del hacking** muestran cómo actúan los atacantes.
  + Herramientas como **FTP, SSH, Nmap, Wireshark y FileZilla** sirven para gestionar y analizar redes.
  + **OWASP** revela los errores comunes en aplicaciones.
  + La **metadata** y el **modelo OSI** permiten identificar riesgos y entender cómo viajan los datos.

## Clase 8 – [04/09/2025]

• Tema central

* Normas y marcos de referencia para la gestión de centros de datos, servicios de TI y riesgos tecnológicos

• **Actividades realizadas**

**NORMA ANSI/TIA-492**  
Es la norma principal para construir un Centro de Datos y es la que establece los requisitos para el diseño, la construcción y la operación de centros de datos, abarcando la infraestructura de telecomunicaciones, arquitectura, sistemas eléctricos y mecánicos para asegurar su fiabilidad y eficiencia

¿Cual es la ultima versión de ITIL?

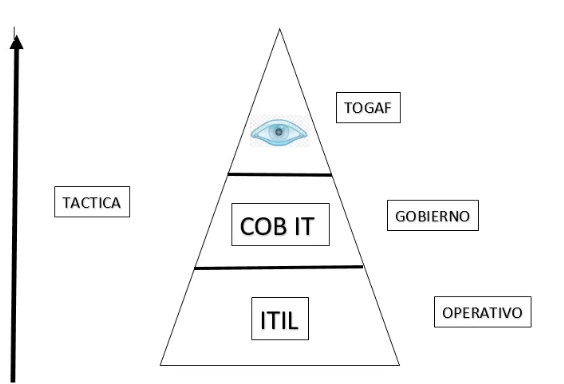
* La última versión de ITIL es **ITIL 4**

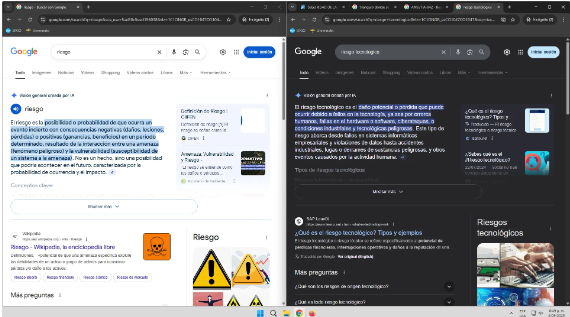
**¿Qué es ITIL 4?**

* Es una actualización significativa respecto a ITIL 3, diseñada para incorporar las tendencias actuales en tecnología y gestión de servicios.
* Se centra en las "[prácticas](https://www.google.com/search?sca_esv=5ad38c5eed156038&rlz=1C1ONGR_esCO1047CO1047&q=pr%C3%A1cticas&sa=X&ved=2ahUKEwjx-ozQvsCPAxU8nWoFHQ0FPOUQxccNegQIExAB&mstk=AUtExfDU0dfmDmholQktnylR0zNdHjMEsiMG5XLY_uKZHLpVVH4wMt3PYCJ90tzxboWUsVta-QgPX4B8siCJLOHJU7rjRrDrZNPebg6XKLiVuO4ydNvXfQmUwoV0vPfiwHrY8jw&csui=3)" en lugar de procesos rígidos, ofreciendo un enfoque más flexible y adaptable a diferentes organizaciones.

**¿Qué es ITIL 4?**

* Es una actualización significativa respecto a ITIL 3, diseñada para incorporar las tendencias actuales en tecnología y gestión de servicios.
* Se centra en las "[prácticas](https://www.google.com/search?sca_esv=5ad38c5eed156038&rlz=1C1ONGR_esCO1047CO1047&q=pr%C3%A1cticas&sa=X&ved=2ahUKEwjx-ozQvsCPAxU8nWoFHQ0FPOUQxccNegQIExAB&mstk=AUtExfDU0dfmDmholQktnylR0zNdHjMEsiMG5XLY_uKZHLpVVH4wMt3PYCJ90tzxboWUsVta-QgPX4B8siCJLOHJU7rjRrDrZNPebg6XKLiVuO4ydNvXfQmUwoV0vPfiwHrY8jw&csui=3)" en lugar de procesos rígidos, ofreciendo un enfoque más flexible y adaptable a diferentes organizaciones.



* Se realizo una breve comparacion entre el riesgo y el riesgo tecnológico  
  Gestión de servicios y recursos en una organización

**Gestión de servicios y recursos en una organización**

* El **ANS/SLA** define la calidad y tiempos de respuesta que un proveedor debe cumplir con un cliente.
* El **OLA** asegura coordinación interna entre equipos para mantener el servicio.
* El **CAPEX** representa inversiones grandes a largo plazo, como equipos o infraestructura.
* El **OPEX** son los gastos diarios necesarios para operar, como sueldos y servicios.

**BIA (Business Impact Analysis / Análisis de Impacto Empresarial)**

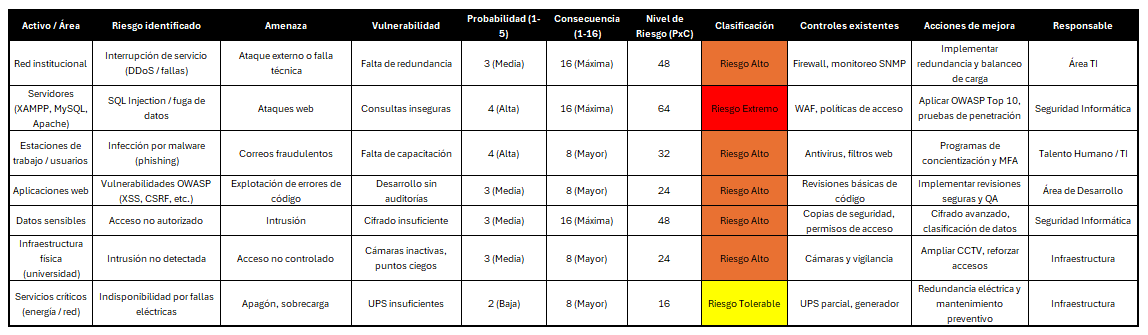
Es un proceso que **detecta las actividades más críticas de una empresa** y analiza qué pasaría si se interrumpen (pérdidas económicas, retrasos, daños a la reputación, etc.).

**TAREA**

* Buscar ejemplos de Matriz y entender q es MATRIZ DE RIESGOS   
  TECNOLOGICOS  
    
  1. Se crea la matriz de riesgos

Captura de pantalla de un juego

El contenido generado por IA puede ser incorrecto.  
2. La **Matriz de Riesgos Tecnológicos** muestra los principales problemas que pueden afectar a la universidad en el uso de la tecnología y la seguridad de la información. En ella se identifican los riesgos, qué los causa, qué debilidades existen, qué tan probables son y qué consecuencias tendrían. También se incluyen las medidas que ya están en uso, las acciones que se pueden tomar para mejorar y quién sería el encargado de hacerlo.



• **Aprendizajes obtenidos:**

* Aprendí que la **gestión de servicios y recursos en una organización** se apoya en acuerdos como el **ANS/SLA** para definir niveles de servicio con clientes y el **OLA** para coordinar equipos internos, mientras que conceptos financieros como **CAPEX y OPEX** ayudan a diferenciar inversiones a largo plazo de los gastos operativos diarios. Comprendí que el **BIA** permite identificar procesos críticos y evaluar el impacto de sus interrupciones, y que la **matriz de riesgos tecnológicos** es clave para analizar amenazas específicas en el ámbito digital. También conocí la **norma ANSI/TIA-492** como guía para el diseño y operación de centros de datos, y la importancia de **ITIL 4** como la versión más reciente de buenas prácticas en gestión de servicios, con un enfoque más flexible y adaptado a las tendencias actuales.

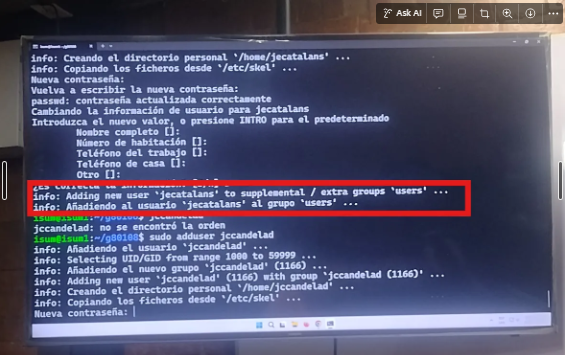
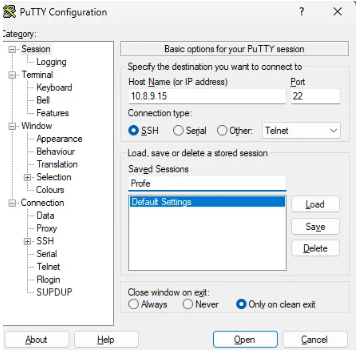
## Clase 9 – [08/09/2025]

• **Tema central**

* Detectar todas las posibles entradas, salidas y puntos de acceso de la UNIMINUTO.

• **Actividades realizadas**  
  
Lo primero que se hizo fue crear mi propio usuario en un cmd en PuTTY desde el equipo del profesor

siguiendo la siguiente estructura

* [Letra Primer Nombre][Letra Segundo Nombre][Primer Apellido][Letra Segundo Apellido]  
    
    
    
  **PuTTY**
* sirve para conectarse de forma remota a computadoras y servidores utilizando protocolos seguros como SSH y Telnet, actuando como un cliente de línea de comandos y emulador de terminal en plataformas Windows
* Instalacion y configuracion del putty al IP LocalHosta 10.8.9.15  
    
    
  Interfaz de usuario gráfica, Texto, Aplicación

  El contenido generado por IA puede ser incorrecto.  
    
  se ingresa el usuario creado anteriormente  
    
    
  Texto

  El contenido generado por IA puede ser incorrecto.
* Lo principal de la clase fue realizar una observación detallada de las afueras de la universidad. Durante este ejercicio, analizamos las posibles entradas y salidas de la institución, así como los puntos de seguridad presentes. También verificamos si las cámaras instaladas cumplen efectivamente su función de vigilancia o si únicamente actúan como elementos de distracción. Además, identificamos los puntos ciegos que podrían representar vulnerabilidades en la seguridad del lugar  
    
  **NORMA DE LOS RIESGOS**  
    
  La **ISO 31000** es una norma internacional que establece principios y directrices para la gestión de riesgos en cualquier tipo de organización. Su propósito es ayudar a identificar, analizar, evaluar y tratar los riesgos de manera estructurada, integrándolos en los procesos y decisiones de la institución.

**Aprendizajes obtenidos:**

* **Creación de usuarios en sistemas remotos**: Aprendí a generar un usuario propio desde la terminal con PuTTY siguiendo una estructura definida.
* **Uso de PuTTY**: Comprendí su función como herramienta para conectarse remotamente a servidores usando protocolos seguros como SSH.
* **Instalación y configuración básica**: Practiqué la conexión con un servidor mediante la IP LocalHost (10.8.9.15).
* **Observación de seguridad en campo**: Identifiqué entradas, salidas, puntos de acceso y posibles vulnerabilidades (cámaras, puntos ciegos, seguridad física) en la universidad.
* **Norma ISO 31000**: Reconocí su importancia como guía internacional para gestionar riesgos, evaluar amenazas y fortalecer la seguridad institucional

## Clase 10– [11/09/2025]

• **Tema central**

* Comandos Basicos de Linux

• **Actividades Realizadas:**

**Bitvise (Software de SSH para Windows)**

Bitvise es un conjunto de herramientas de software (Bitvise SSH Client y Bitvise SSH Server) diseñado para proporcionar conexiones seguras y transferencia de datos en sistemas Windows.

INSTALACION

* Se instala la aplicación Cliente  
  Una captura de pantalla de una computadora

  El contenido generado por IA puede ser incorrecto.
* Se aceptan los Terminos y Condiciones para llevar acabo la instalación  
  Interfaz de usuario gráfica, Texto, Aplicación

  El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

Despues de finalizada la instalación de la aplicación, se ingresa de manera Local al servidor que en este caso su Direccion ipv4 es 10.8.9.15 y se ingresa de igual forma el usuario creado anteriormente   
  
  
Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.  
Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.  
  
  
- Los principales métodos para la gestión FTP son el uso de modos de conexión (activo y pasivo) para la transferencia de datos, la utilización de comandos FTP como ABOR, ASCII o BINARY para controlar la sesión, y la aplicación de herramientas de software cliente como FileZilla o WinSCP para interactuar con el servidor  
  
Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.  
- se cierra el proceso de manera correcta para no dejarlo huerfano  
Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.  
  
**COMANDOS DE LINUX**

* ls - Nos fijamos que tenemos no mas un directorio

Texto

El contenido generado por IA puede ser incorrecto.  
  
Creacion de un objeto, que pueda ser ejecutado con un serie de orndenes en linux y en windows  
  
**WINDOWS**

* Creacion de un archivo de texto  
  Una captura de pantalla de un celular

  El contenido generado por IA puede ser incorrecto.
* Escribir una orden en el archivo creado por distraccion y se guarda  
  Interfaz de usuario gráfica, Texto, Aplicación

  El contenido generado por IA puede ser incorrecto.
* se le cambia la extension al archivo por .bat o si es win11 por .ps1

Una captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

**LINUX**

Texto

El contenido generado por IA puede ser incorrecto.

* para saber en que directorio estoy ubicado y para que sepamos en que servidor estamos  
  Interfaz de usuario gráfica, Texto

  El contenido generado por IA puede ser incorrecto.

• **Aprendizajes obtenidos:**

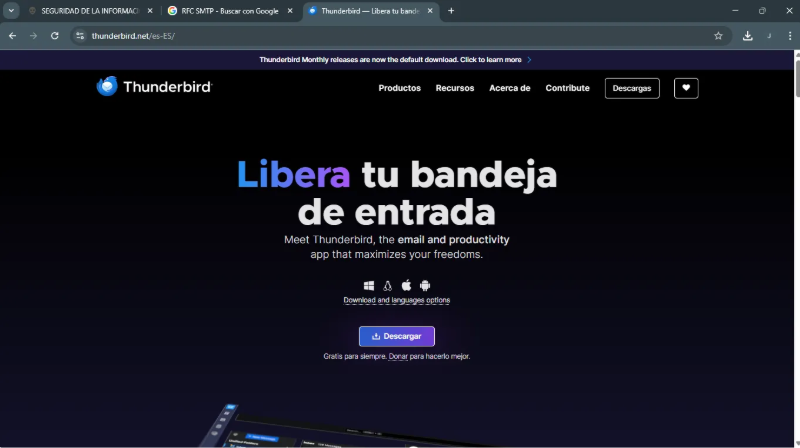
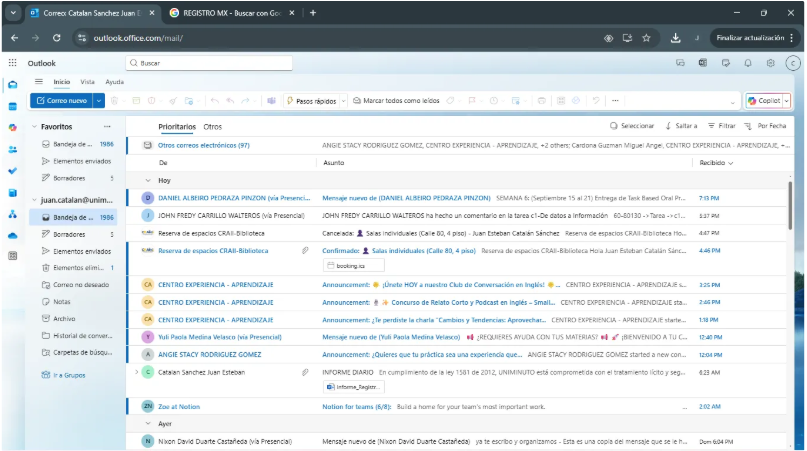
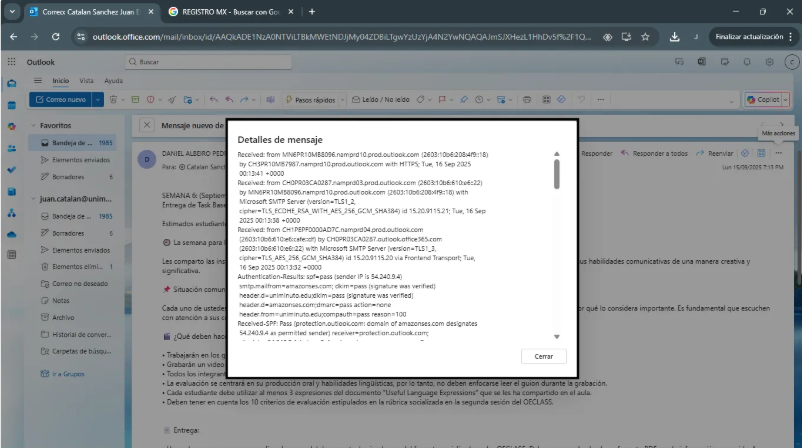
* **Bitvise SSH**: Comprendí cómo instalar y usar este cliente para establecer conexiones seguras y gestionar accesos a un servidor remoto.
* **FTP**: Identifiqué los modos de conexión (activo y pasivo), comandos básicos y herramientas como FileZilla o WinSCP para transferencias de datos.
* **Comandos Linux**: Aprendí a usar comandos iniciales como ls y a verificar el directorio y servidor en uso.
* **Automatización**: Practiqué la creación de archivos ejecutables en Windows (.bat o .ps1) y objetos en Linux para ejecutar órdenes.
* **Buenas prácticas**: Reconocí la importancia de cerrar procesos correctamente para evitar que queden huérfanos.

## Clase 10– [11/09/2025]

• **Tema central**

* Protocolo para manipular buzón SMTP (envío y análisis de correos electrónicos).

• **Actividades realizadas**  
  
Revisión teórica del protocolo SMTP: definición, RFCs y puerto por defecto (25).

* Revisión y comparación con IMAP (función y diferencias frente a SMTP).
* Configuración/uso de cliente de correo: Thunderbird (apuntar que se usó Thunderbird como cliente de pruebas).  
    
  
* Ingreso al correo vía Microsoft (web/Outlook) para replicar y copiar el detalle del correo.  
    
  
* Copiado del detalle del correo (headers, remitente, rutas, timestamps).  
    
  
* Análisis de cabeceras del correo usando mxtoolbox (Header Analyzer) para identificar origen, rutas y posibles problemas.  
    
  Imagen que contiene Gráfico

  El contenido generado por IA puede ser incorrecto.  
  Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

  El contenido generado por IA puede ser incorrecto.
* Uso del OSINT Framework para guiar la investigación de fuentes y herramientas adicionales relacionadas con correos y dominios.

• **Aprendizajes obtenidos:**Entendí qué es SMTP y por qué es el estándar para enviar correos entre servidores (y que las RFCs definen su comportamiento).

* Diferenciación práctica entre SMTP (envío) e IMAP (recepción/sincronización)
* Aprendí a extraer y leer cabeceras de correo: qué campos buscar (Received, From, Return-Path, SPF, DKIM, DMARC, Message-ID, timestamps)
* Cómo usar mxtoolbox para analizar cabeceras y registros MX; qué información útil entrega (servidores receptores, listar rutas, detectar rebotes o reenvíos sospechosos).
* Uso del OSINT Framework como guía para herramientas complementarias y metodología de investigación.
* Comprendí la importancia del registro MX en la entrega de correo y cómo afecta la recepción de mensajes.
* Buenas prácticas al documentar un taller: capturas, pasos reproducibles y separar evidencias (pantallazos) de análisis.
* Consideraciones de seguridad y éticas al manipular/analizar correos (no divulgar datos sensibles, respetar privacidad).

# 5. Conclusiones

A lo largo del desarrollo de las clases se consolidaron aprendizajes fundamentales sobre la **seguridad de la información**, el uso de **protocolos y herramientas de red**, así como la aplicación de **normas y marcos de referencia internacionales**. Se logró reconocer la importancia de conceptos como **CIA/DIC, ISO 27001, ISO 31000 e ITIL 4**, que constituyen bases esenciales para la gestión de la seguridad en las organizaciones.

En el ámbito práctico, el uso de programas como **PuTTY, Bitvise, MobaXterm, Nmap, Wireshark, FileZilla y Advanced IP Scanner** permitió afianzar competencias técnicas en el manejo de conexiones seguras, escaneo de redes, gestión de usuarios y análisis de vulnerabilidades. Asimismo, el desarrollo de ejercicios de **SQL Injection, gestión de inventarios en bases de datos y automatización mediante scripts** reforzó la capacidad de identificar riesgos y aplicar medidas de protección en entornos controlados.

Las observaciones en campo, como la identificación de **puntos de acceso y vulnerabilidades físicas en la universidad**, complementaron la formación teórica, mostrando que la seguridad no se limita a lo digital, sino que integra también aspectos físicos y organizacionales.

En conclusión, el curso permitió fortalecer una visión integral de la seguridad de la información, entendida no solo como un requisito académico, sino como una competencia profesional y personal necesaria para enfrentar los retos actuales en materia tecnológica y de protección de datos.

# Bibliografía

* ANSI/TIA-492. (2019). *Optical Fiber Cabling Components Standard*. Telecommunications Industry Association.
* ISO. (2018). *ISO/IEC 27001:2013 – Information technology — Security techniques — Information security management systems — Requirements*. International Organization for Standardization.
* ISO. (2018). *ISO 31000:2018 – Risk management — Guidelines*. International Organization for Standardization.
* Axelos. (2019). *ITIL® 4: Foundation*. London: TSO (The Stationery Office).
* OWASP Foundation. (2021). *OWASP Top 10 – Ten Most Critical Web Application*