Centro de
Investigación en
Computación

Ciberseguridad

Definiciones

Background

Course

Ciberseguridad

Instructor

Acosta Bermejo Raúl

Lecture notes

2025-A
Febrero del 2025
Última actualizacioón

Instituto
Politécnico
Nacional

Table of contents (outline)

Tabla de contenido

1. Introducción
2. Conceptos básicos
3. Diseño de la seguridad
4. Varios temas y resumen

Introducción

Definiciones

Introducción

Aclaraciones

Evolución de términos

1. Ciber
   - RAE. Indica relación con redes informáticas.
   - Ciencia que estudia las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas.
   - Diccionarios en inglés: Adj. *involving, using, or relating to computers, especially the internet*.
2. Etimología y orígenes
   - El matemático norteamericano Norbert Wiener acuñó el término en 1948 en "*Theory or study of communication and control*".
   - El primero en usarlo en Ciencia ficción y popularizarlo fue William Gibson, con el término *cyberspace* en historia corta "*Burning Chrome*". Mas tarde en los 80s Gizmodo uso el término futurístico *cyberpunk*.
3. Otros términos
   - Cibernético, ciberfísico, ciberespacio, cibernauta, ciberdelincuente, ciberguerra, etc.

Conceptos

Definiciones

Objetivos / Afectación

Ciberseguridad (cybersecurity)

1. NIST
   - The process of protecting **information** by preventing, detecting, and responding to attacks.
   - Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
   - Measures and **controls** that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.
2. Wikipedia Inglés
   - Computer security (also cybersecurity, digital security, or information technology (IT) security) is the protection of computer software, systems and networks from threats that can lead to unauthorized information disclosure, theft or damage to hardware, software, or data, as well as from the disruption or misdirection of the services they provide.
3. CISA (Agencia de EU)
   - It is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. It seems that everything relies on computers and the internet now: communication, entertainment, transportation, shopping, medicine, and the list goes on.

Conceptos

Definiciones

Ciberseguridad (cybersecurity)

Ver otras definiciones de empresas:

1. Kaspersky
   - https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security?srsltid=AfmBOopout9-D0uhSYmibkUuAX7VEOO2HhHrmLi9alx1hVThIXEnBKWG
2. Amazon
   - https://aws.amazon.com/es/what-is/cybersecurity/
3. IBM
   - https://www.ibm.com/mx-es/topics/cybersecurity
4. Microsoft
   - https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-la-ciberseguridad-8b6efd59-41ff-4743-87c8-0850a352a390
5. Fortinet
   - https://www.fortinet.com/lat/resources/cyberglossary/what-is-cybersecurity
6. SCITUM
   - https://resources.scitum.com.mx/wp-content/uploads/2018/02/WP-QUE-ES-LA-CIBERSEGURIDAD-resources.pdf

Conceptos

Definiciones

¿Que se protege?

Conceptos

Definiciones

Criptografía Infraestructura
Implementaciones

Propiedades / Implementación

- Confidencialidad / Cifrado[Cripto]
- Integridad / Funciones Hash[Cripto] (FH)
- Autenticación / Firmas digitales[Cripto] (FD = FH y Sistemas)

  Consistente en poder verificar que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Violaciones de esta propiedad son la manipulación del origen o el contenido de los datos y en el caso de los usuarios o servicios se da la Suplantación de Identidad.
- No repudio / Pruebas de integridad y origen de los datos (FD en Certificados)

  Se refiere a un estado de negocios donde el supuesto autor de una declaración no es capaz de desafiar con éxito la validez de declaración o contrato. El término es a menudo visto en un entorno legal donde la autenticidad de una firma está siendo desafiada.
- Disponibilidad / Redundancia[Infra]

  Disposición de los servicios a ser usados cuando sea necesario. Ataques buscan la Interrupción del Servicio y su productividad.
- Trazabilidad / Bitacoras[Infra]

  Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilida materializa en la integridad de los registros de actividad.
- Resiliencia, …

Conceptos Básicos

Definiciones

Conceptos

Definiciones

Lista

1. Amenaza / Threat
2. Riesgo / Risk
3. Ataque / Attack
4. Debilidad / Weakness
5. Vulnerabilidad / Vulnerability
6. Explotación / Exploit
7. Incidente de Seguridad / Security Incident
8. Brecha de seguridad / Breach

Conceptos

Definiciones

Quien
Objetivo (target)
Daño

Amenaza / Threat

- NIST definition

  Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

- Wikipedia definition.

  It is a potential negative action or event facilitated by a vulnerability that results in an unwanted impact to a computer system or application. A threat can be either:

  - A negative "intentional" event: i.e. hacking: an individual cracker or a criminal organization.
  - An "accidental" negative event: e.g. the possibility of a computer malfunctioning, or the possibility of a natural disaster event such as an earthquake, a fire, or a tornado.
  - Otherwise a circumstance, capability, action, or event.

Conceptos

Definiciones

probability vs likelihood

Riesgo / Risk

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

- NIST definition

  A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

- Actividades
  - Análisis: Identificar los riesgos.
  - Evaluación (*Risk assesment*): Calcular la probabilidad.
  - Gestión: Que hacer para prevenirlos, mitigarlos (elim)
- Estándares
  - MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), Versión 3.

Conceptos

Definiciones

Ataque / Attack

- NIST definition

  Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

- Varias clasificaciones de los Tipos de ataque. La más sencilla:
  - Al sistema operativo.
  - A un error de configuración.
  - A una aplicación.
- Estándar
  - https://attack.**mitre**.org/ Muy completa (extensa)

Conceptos

Definiciones

Debilidad / Weakness

- NIST definition

  Defect or characteristic that may lead to undesirable behavior.
- Estándar
  - Uno de los más conocidos y completos:

    https://cwe.**mitre**.org/
  - La mayoría son en software pero tambien contempla en hardware, configuración, etc.

Conceptos

Definiciones

A flaw (defecto) is unintended functionality. This may either be a result of poor design or through mistakes made during implementation.

Vulnerabilidad / Vulnerability

- NIST definition

  Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

- NCSC definition

  It is a weakness in an IT system that can be exploited by an attacker to deliver a successful attack. They can occur through flaws, features or user error, and attackers will look to exploit any of them, often combining one or more, to achieve their end goal.

- Estándares
  - CVSS (Common Vulnerability Scoring System) creado por el NIST y aplicado en NVD (National Vulnerability Database).

    It is a method used to supply a qualitative measure of severity. CVSS is not a measure of risk. CVSS consists of three metric groups: Base, Temporal, and Environmental.

Conceptos

Definiciones

Vulnerability Vs Weakness

- Weaknesses and vulnerabilities are both states that indicate security risks.
- While weakness refers to an application error or bug, it may escalate to a vulnerability in cases where it can be exploited to perform a malicious action.
- The difference between a weakness and a vulnerability is the availability of a specific payload allowing it to be exploited.
- Once an exploit is available it is considered a confirmed vulnerability and as such it holds greater risk to the application security.

All vulnerabilities rely on weaknesses,

but not all weaknesses entail vulnerabilities.

Conceptos

Definiciones

Explotar, aprovechar / Exploit

- Es un programa informático, una parte de un software o una secuencia de comandos que se aprovecha de un error o vulnerabilidad para provocar un comportamiento no intencionado o imprevisto en un software, hardware o en cualquier dispositivo electrónico.
- Estos comportamientos incluyen, por lo general, la toma del control de un sistema, la escalación de privilegios, etc.
- Las vulnerabilidades de Día Cero (también conocidas como 0-day exploits) son las brechas de seguridad en el software desconocidas hasta el momento del ataque.

Conceptos

Definiciones

Jeopardizes
Daño (noun)
Comprometer (verb)

Incidente de Seguridad / Security Incident

- NIST definition

  An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

- Propiedades en Seguridad
  - Criptografía

    Confidentiality, Integrity, Authentication, Non-repudiation

    Cifrado F. Hash. Digital signatures **Implementaciones**
  - Infraestructura

    Availability

Accountability

Propiedad de un recurso del sistema que asegura que las acciones de una entidad del sistema puedan ser rastreadas sin ambiguedad, lo que la hace responsable de sus acciones.

Conceptos

Definiciones

Brecha de seguridad / Breach

- *It is any incident that results in unauthorized access to computer data, applications, networks or devices*.
- Una brecha de seguridad es “un incidente de seguridad que afecta a datos de carácter personal” y que, además, puede ocasionar la “destrucción, pérdida, alteración accidental o ilícita de los datos personales transmitidos, conservados o tratados, así como la comunicación o el acceso no autorizados a los mismos.” Fuente AEPD (España).
- Con independencia de si se ha originado como consecuencia de un accidente o si se trata de una acción intencionada y de que afecte a datos en formato digital o en formato papel.
- Un incidente puede tratarse, por ejemplo, de una infección con malware o un ataque DDOS. No supone el acceso a la red ni la pérdida de datos. Por lo tanto, no lo podemos considerar brecha de seguridad.

https://www.kaspersky.com/resource-center/threats/what-is-a-security-breach

Conceptos

Definiciones

Contramedidas / Countermeasure

- Actions, devices, procedures, or techniques that meet or oppose (i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.
- Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.

Conceptos

Definiciones

Resumen

Los conceptos anteriores se relacionan de la siguiente forma:

Weakness => Vulnerability => Exploit => Security Incident => Security breach
=> Security Event
=> Threat

Conceptos

Definiciones

Varios conceptos

- Cracking
  - Es un parche creado sin autorización del desarrollador del programa al que modifica cuya finalidad es la de modificar el comportamiento del *software* original.
  - Password cracking tools.
- Privilege escalation
  - It is the act of exploiting a bug, a design flaw, or a configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.
  - *Jailbreaking* is defined as the act of removing limitations that a vendor attempted to hard-code into its software or services.

Conceptos

Definiciones

Varios conceptos

- Campaigns
  - An individual or group involved in malicious cyber activity is called a **Threat Actor**.
  - A set of activity (Incidents) carried out by Threat Actors using specific techniques (TTP) for some particular purpose is called a **Campaign**. Such activity might fit along the lines of stealing financial information from banking customers or targeting a particular business sector.
  - https://stixproject.github.io/documentation/idioms/campaign-v-actors/

Conceptos

Definiciones

Servicios en la Nube

- Tipos
  - Software as a Service (SaaS) Aplicaciones
  - Platform as a Service (PaaS) Sistema Operativo, BD, etc
  - Infrastructure as a Service (IaaS) Hardware, Servidores, Switches
- Para el malware existe:
  - Malware as a Service (MaaS)
  - Ransomware a Service (RaaS)

Conceptos

Definiciones

Hacker

BlackHat

Ejemplos

- Lizard Squad

  4 cracker que atacaron la industria del Videojuego a partir del 2014 usando DDoS.

- Anonymous
  - http://www.anonops.net/
- Ciberactivismo

Conceptos

Definiciones

Modelo de Madurez de la Cibereguridad

Visión holística de la ciberseguridad

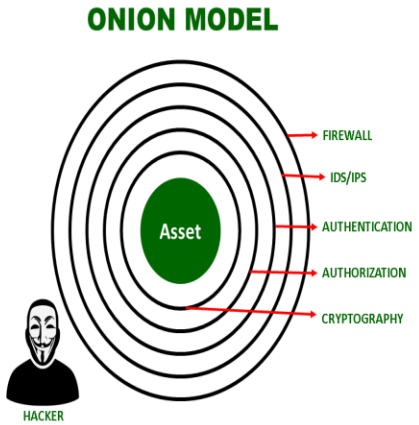
- Activos
  - Software y Equipamiento
- Capacitación y certifiaciones
- Auditorias

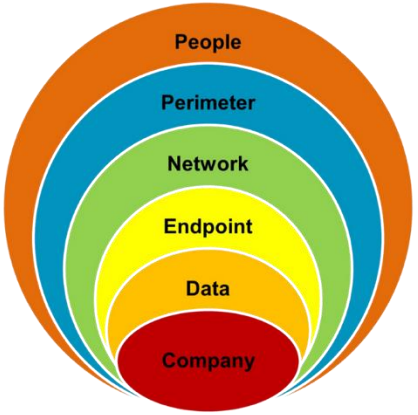
Conceptos

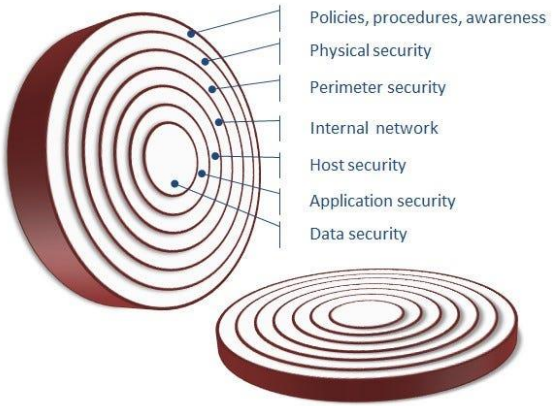
Definiciones

Modelo de Seguridad a Capas (cebolla)

Dimensiones, capas, dominios, etc





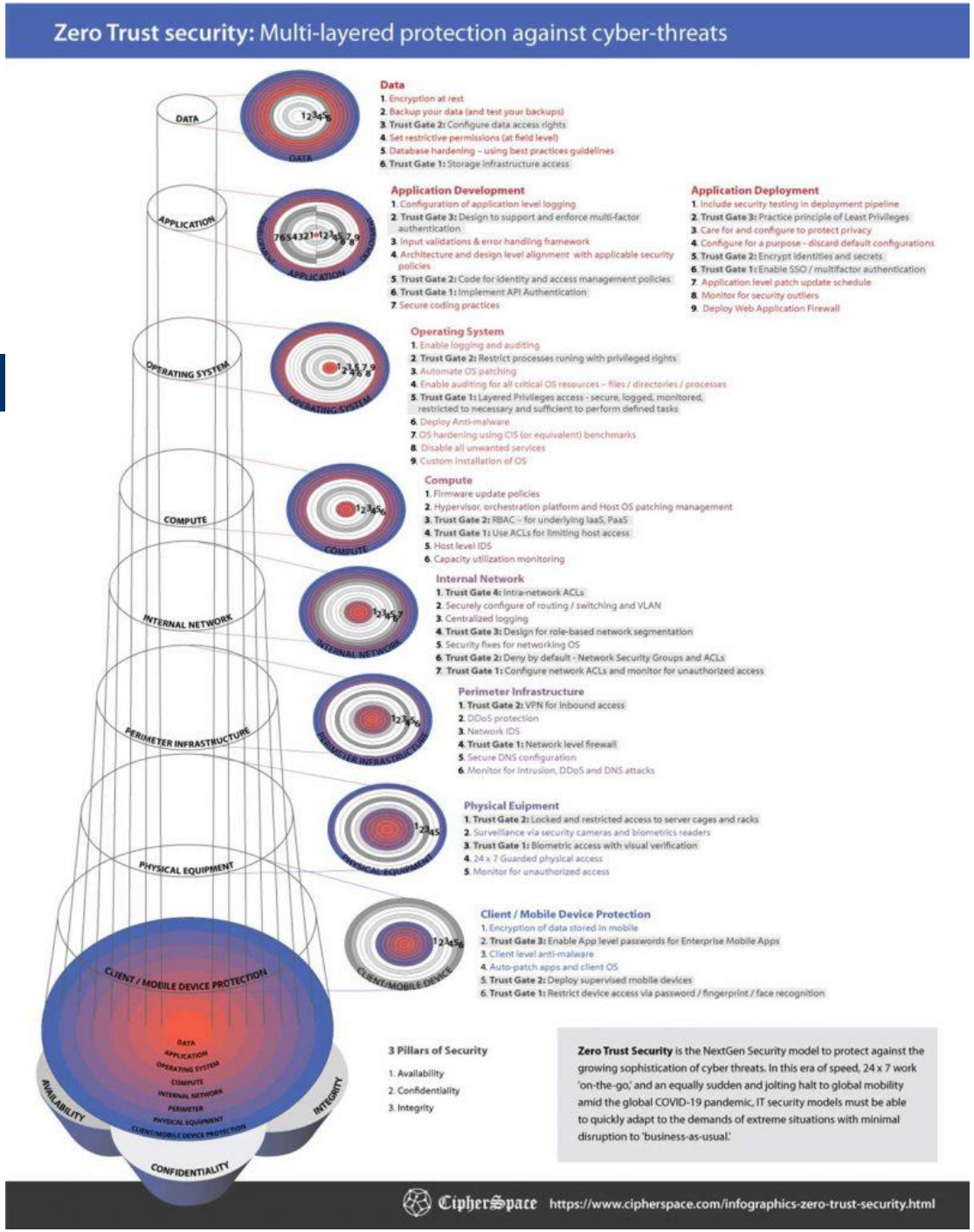


Conceptos

Definiciones

OSI model layers

Host layers	7	Application layer	Exploit
	6	Presentation layer	Phishing
	5	Session layer	Hijacking
	4	Transport layer	Reconnaissance / DoS
Media layers	3	Network layer	Man-in-the-middle
	2	Data link layer	Spoofing
	1	Physical layer	Sniffing



Diseño de la Seguridad

Definiciones

Conceptos

Definiciones

Ciclo de Vida del Desarrollo de Software

1. Análisis: Requerimientos
2. Diseño: Diagramas, Casos de Uso
3. Implementación: Código
4. Pruebas: Plan, Casos de Prueba y Evid.
5. Documentación
6. Despliegue: Configuración
7. Mantenimiento: Reportes

Cascada, espiral, prototipos, etc.
Frameworks: Rup, Scrum, Agile, SAFe, Xp, Kanban.
Srumban = S + K
DevOps, DevSecOps

Requerimientos

- Funcionales
  - Operaciones, se describen con Casos de Uso.
- No funcionales
  - Propiedades, medibles.
  - Portable, Multiplataforma cumplimiento de estándares.
- Otras clasificaciones
  - Usabilidad (experiencia de usuario, ergonomía)
  - Estress
  - Volumetría.
  - Tolerancia a fallas.

Reglas de Negocio.

Diseño de la

Seguridad

Requerimientos de Seguridad

1. R. de Hw
2. R. de Sw
   i. Análisis de Vulnerabilidades
3. R. de Procesos de Negocio
4. Controles de Seguridad
   i. Control de Acceso
      - De usuarios, de entidades/components que se comunican (API REST).

      ¿Que modelo usar? RBAC, ABAC, etc.
   ii. .

Diseño de la

Seguridad

Lista

1. Políticas
2. Mecanismos
3. Controles
4. Procedimientos

Políticas
↓
Procedimientos
↓
Controles

Conceptos

Definiciones

Policy[NIST]

Statements, rules or assertions that specify the correct or expected behavior of an entity. For example, an authorization policy might specify the correct access control rules for a software component.

- Políticas
  - Son un conjunto de reglas o afirmaciones (*assertions*) que definen cómo proteger los sistemas y la información de una organización.
  - Deben ser aprobadas por la dirección de la organización y comunicadas a todo el personal.
  - Definen **Qué** se debe proteger y **Cómo**.
- Controles de seguridad
  - Son las medidas que se implementan para hacer cumplir las políticas.
  - Cualquier tipo de protección o contramedida utilizada para evitar, detectar, contrarrestar o minimizar los riesgos de seguridad de la propiedad física, la información, los sistemas informáticos u otros activos.
  - Pueden ser preventivos, detectivos, defensivos o correctivos.
- Mecanismos de seguridad
  - Son herramientas técnicas y métodos técnicos que se utilizan para implementar los servicios de seguridad.

Conceptos

Definiciones

Políticas Reglas o Afirmaciones Que	**Controles** Como	**Mecanismos** Implementan las Políticas
	Pueden ser: Técnicos, administrativos y físicos	Tecnologías, Procesos y procedimentales
Políticas de acceso	Control de acceso	Sistemas de autenticación
Clasificación de datos		Firewalls

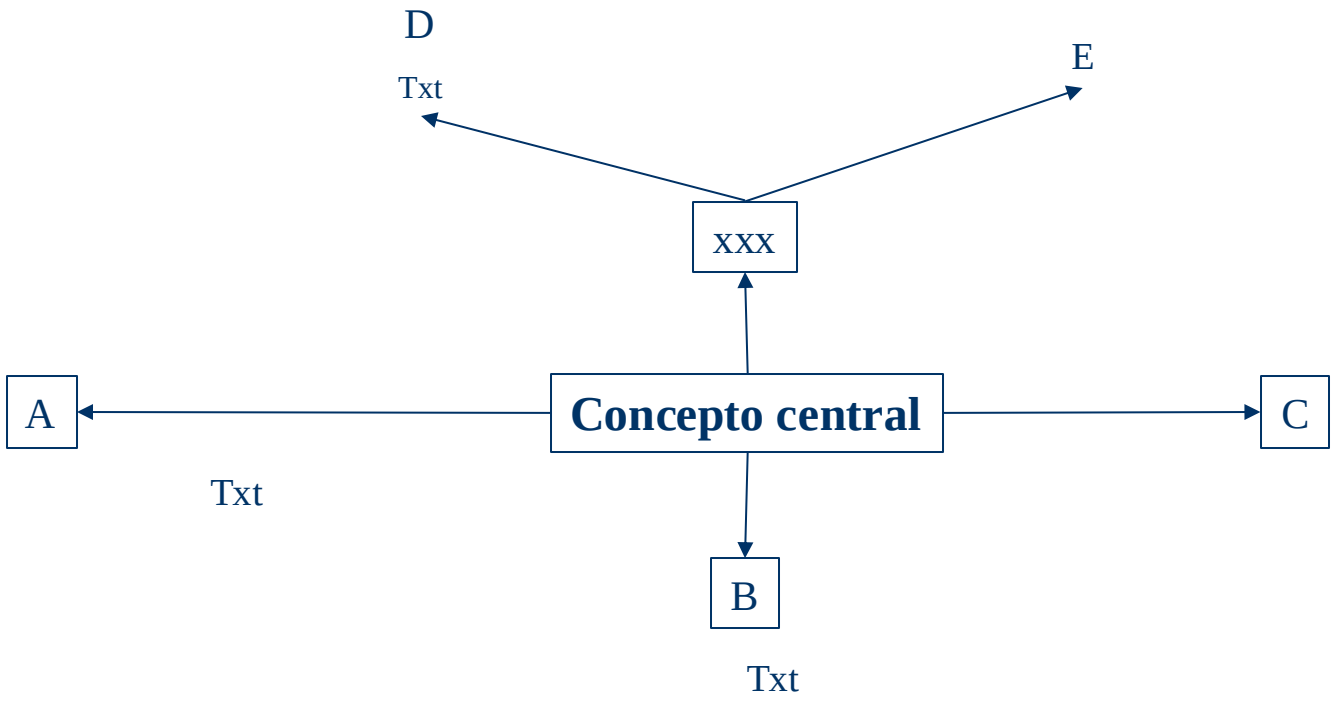
Controles Mecánicos
Físicos

Varios temas

Y resumen

Mapa mental

Resumen



The end

Contacto

Raúl Acosta Bermejo

http:www.cic.ipn.mx
http://www.ciseg.cic.ipn.mx/

racostab@ipn.mx
racosta@cic.ipn.mx

57-29-60-00
Ext. 56652