Guardia Civil

Mando de Apoyo

Jefatura de Servicios Técnicos

SEGURIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

CLASE 2

PRINCIPIOS BÁSICOS DE LA CIBERSEGURIDAD

Capitán GC
Jesús S. Cano Carrillo

ACADEMIA DE INGENIEROS

Estado de Alarma, 12 de mayo de 2020

PRINCIPIOS BÁSICOS DE LA CIBERSEGURIDAD

- En esa clase, se verá las definiciones, dimensiones y principios básicos de la ciberseguridad.

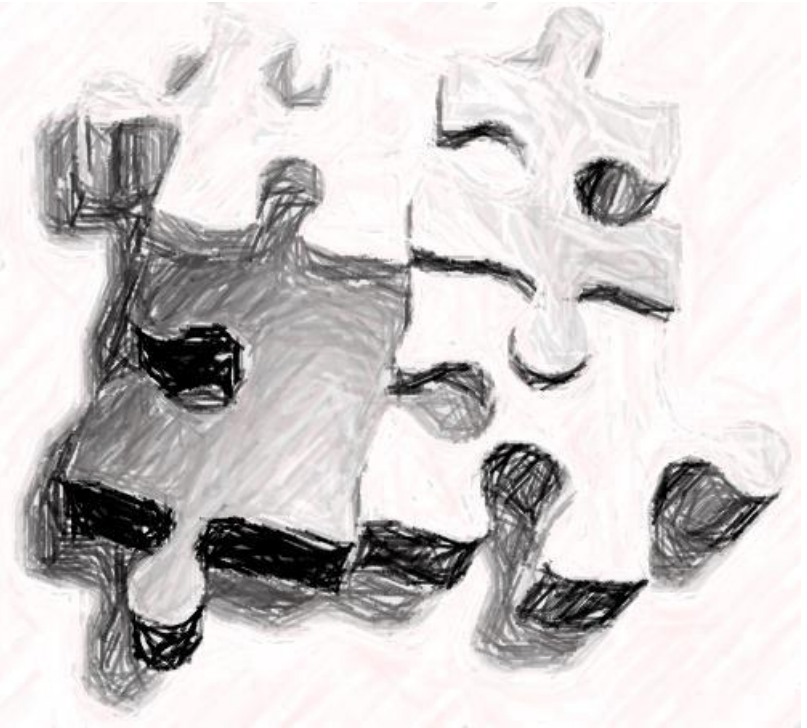
Due to Coronovirus (COVID19) all TCP applications have to be converted to UDP to avoid Handshakes

DOS FORMAS DE VER LA CIBERSEGURIDAD

- ¿Cuál es tu opinión?

Cuestión de nomenclatura

- SEGURIDAD DE LA INFORMACIÓN
- SEGURIDAD INFORMÁTICA
- SEGURIDAD DE LAS TIC (en inglés, ICT)
- CIBERSEGURIDAD



Definición de ciberseguridad

- Conjunto de
  - **herramientas,**
  - **políticas,**
  - **conceptos de seguridad,**
  - **salvaguardas de seguridad,**
  - **directrices (guidelines),**
  - **métodos de gestión de riesgos,**
  - **acciones,**
  - **formación,**
  - **prácticas idóneas (best practices),**
  - **seguros (assurance)**
  - **y tecnologías**

que pueden utilizarse para proteger a los activos de la organización y a los usuarios en el ciberentorno.

(Definición de la UIT-T, X.1205: Aspectos generales de la ciberseguridad, 2008)

Recomendación ITU

3.2.5 ciberseguridad: El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes:

- disponibilidad;
- integridad, que puede incluir la autenticidad y el no repudio;
- confidencialidad.

6

Otras definiciones

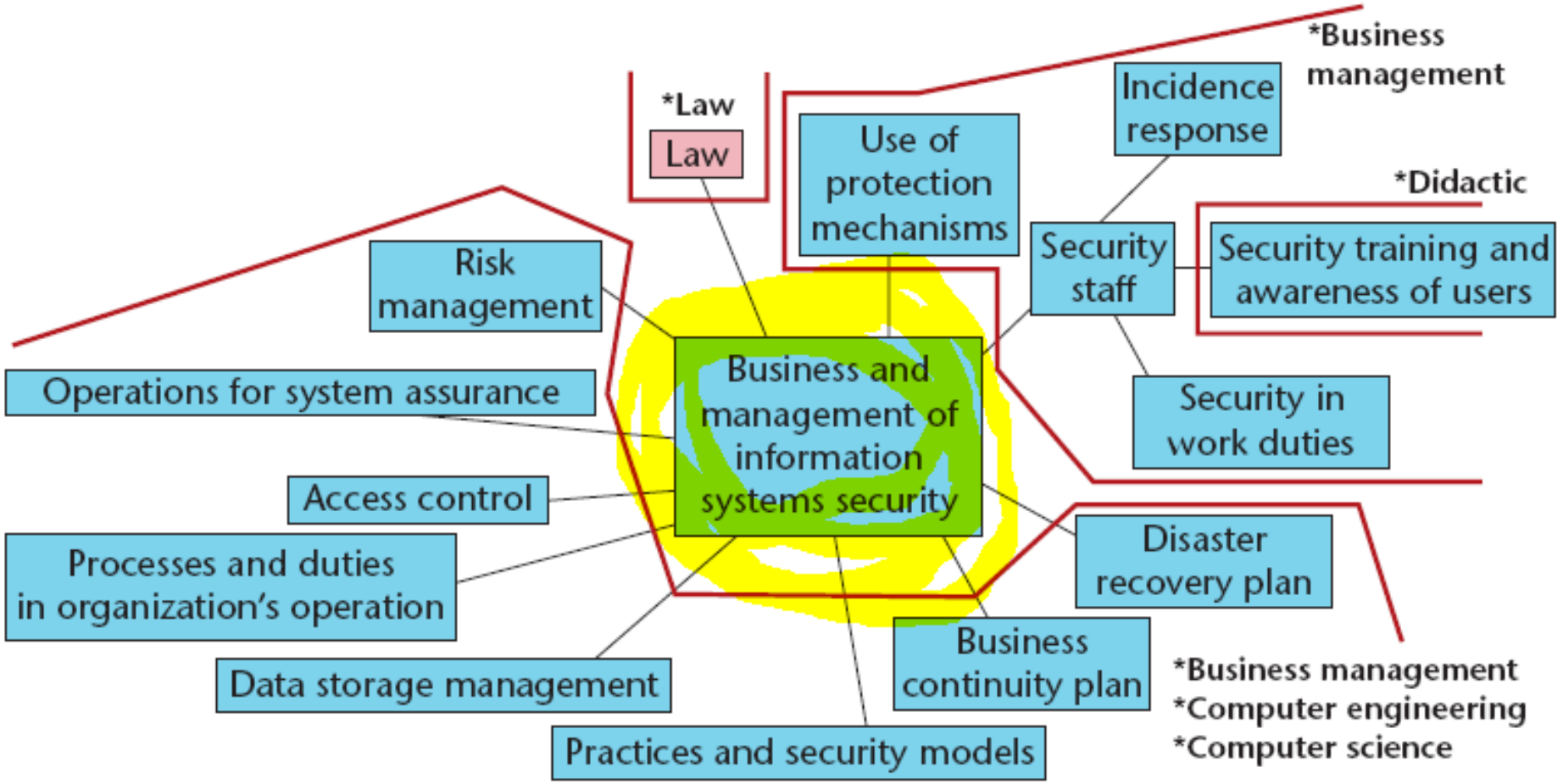
- La **seguridad de la información** es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos

que permitan resguardar y proteger la información

buscando mantener la confidencialidad,
la disponibilidad e integridad de la misma.

7

El contexto multidisciplinar STIC



FUENTE: Common Body of Knowledge for Information Security, 2007 [2]

8

Tareas más relevantes

Information security task*
1. Assess security risks of information assets
2. Interact with information security product and service vendors or customers
3. Educate and train users regarding information security
4. Develop organizational information security policies and guidelines
5. R&D (secure network, cryptology, security devices, and so on)
6. Ensure all system users comply with the organizational information security policy
7. Intelligence and information gathering in the information security community
8. Design and implement access controls
9. Audit and monitor user access and identify security events
10. Investigate information security incidents
11. Enforce information security in software design and development
12. Install and manage security equipments and software
13. Develop the business continuity plan
14. Encrypt and decrypt classified information
15. Recover business operations in response to security events
16. Implement physical protection for information system resources
17. Prosecute unlawful users or information system abusers

FUENTE: Estudio entre profesionales de la seguridad, 2010 [04]

9

Dimensiones de la seguridad

- Dimensiones u objetivos básicos, o propiedades, de la información o los sistemas de información.

✓CONFIDENCIALIDAD.

Propiedad que protege la información del acceso de personas no autorizadas.

✓INTEGRIDAD.

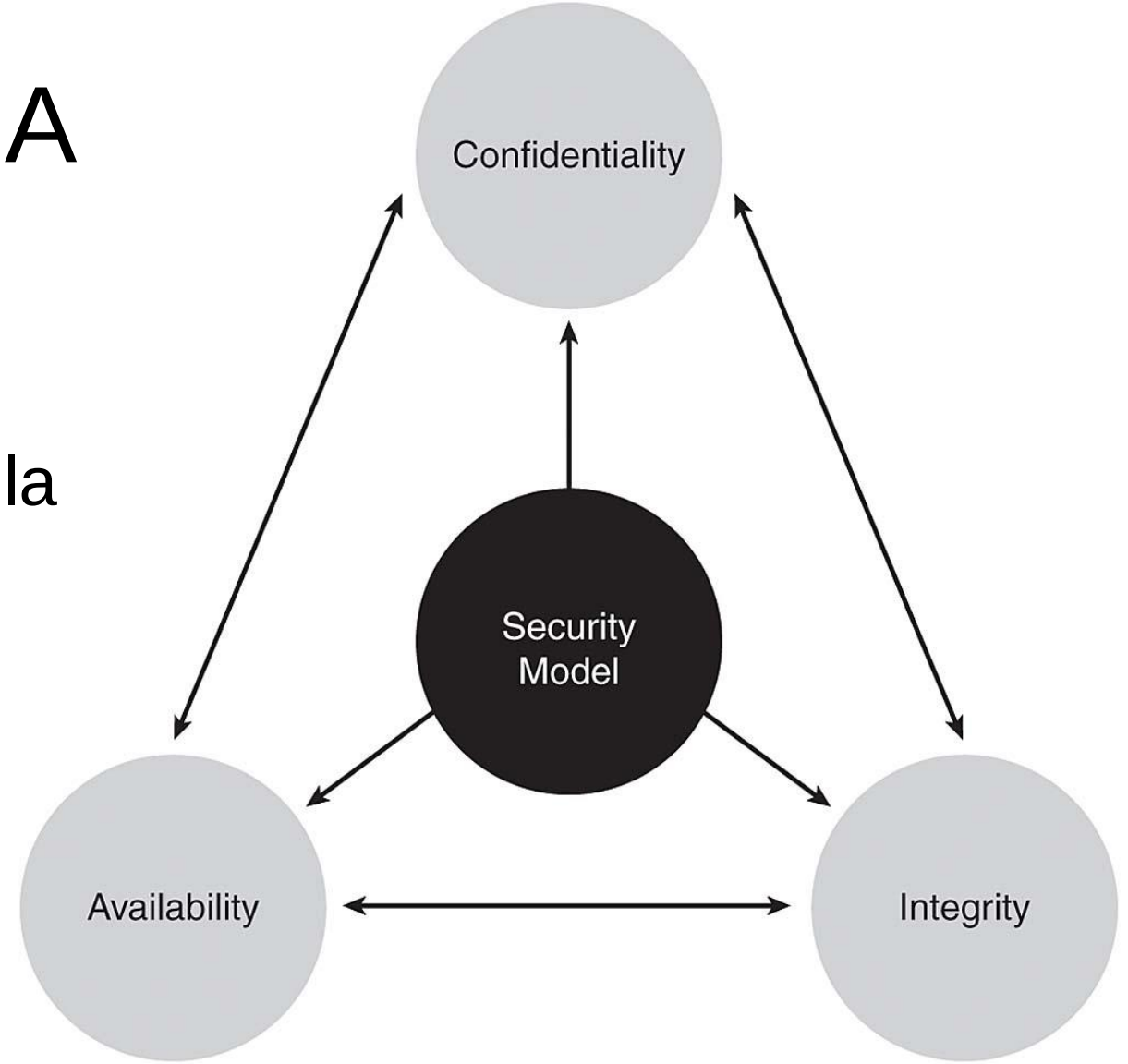
Propiedad que protege la información de modificaciones/eliminaciones no autorizadas.

✓DISPONIBILIDAD.

Propiedad que protege el uso, oportuno y fiable, de la información. (Availability)

Triángulo CIA

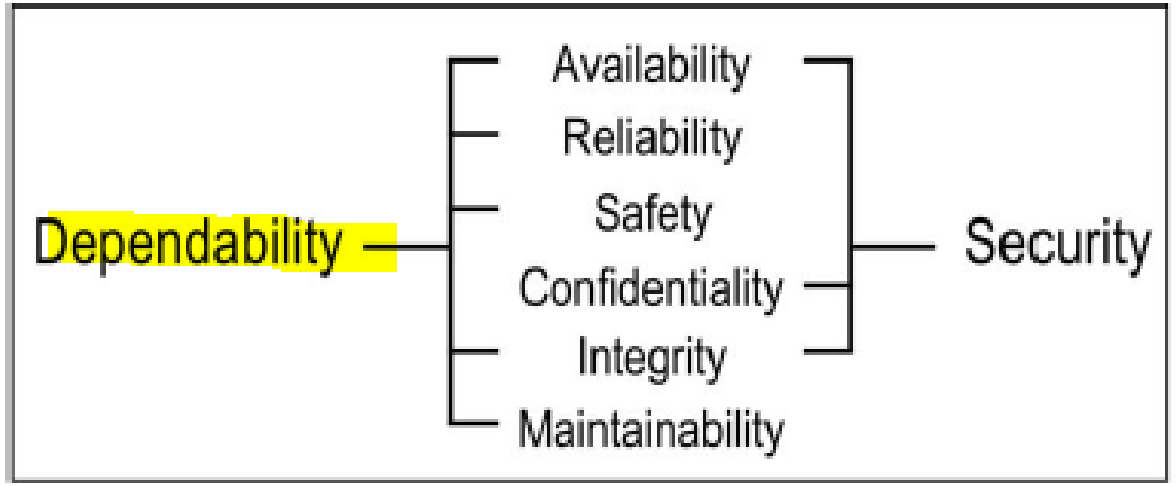
- Modelo de seguridad de la información



11

El modelo de confianza de la información

- CONFIANZA (Dependability)
  - Disponibilidad (corrección)
  - Fiabilidad (continuidad)
  - Seguridad (safety: accidentes, peligros)
  - Confidencialidad
  - Integridad
  - Mantenibilidad

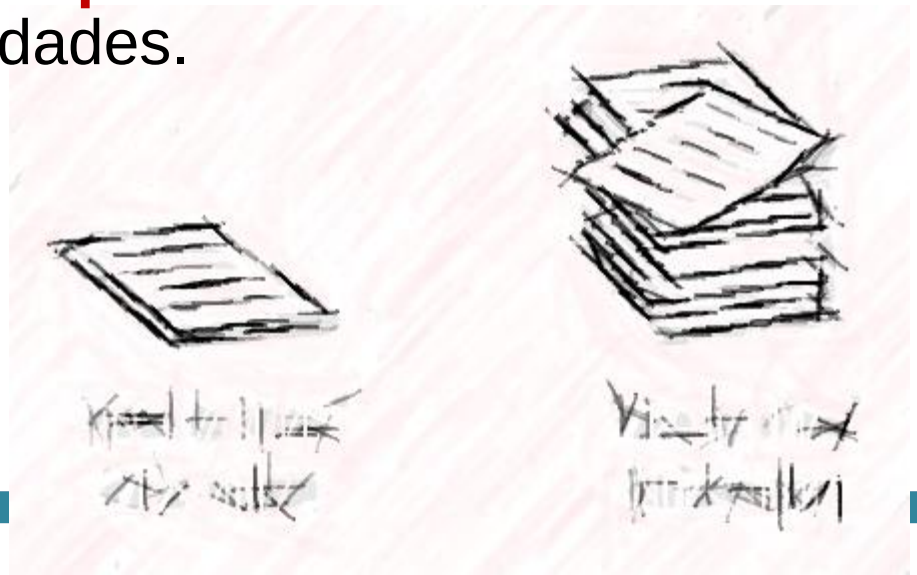


Dependability and security attributes.

12

Principio de la necesidad de conocer

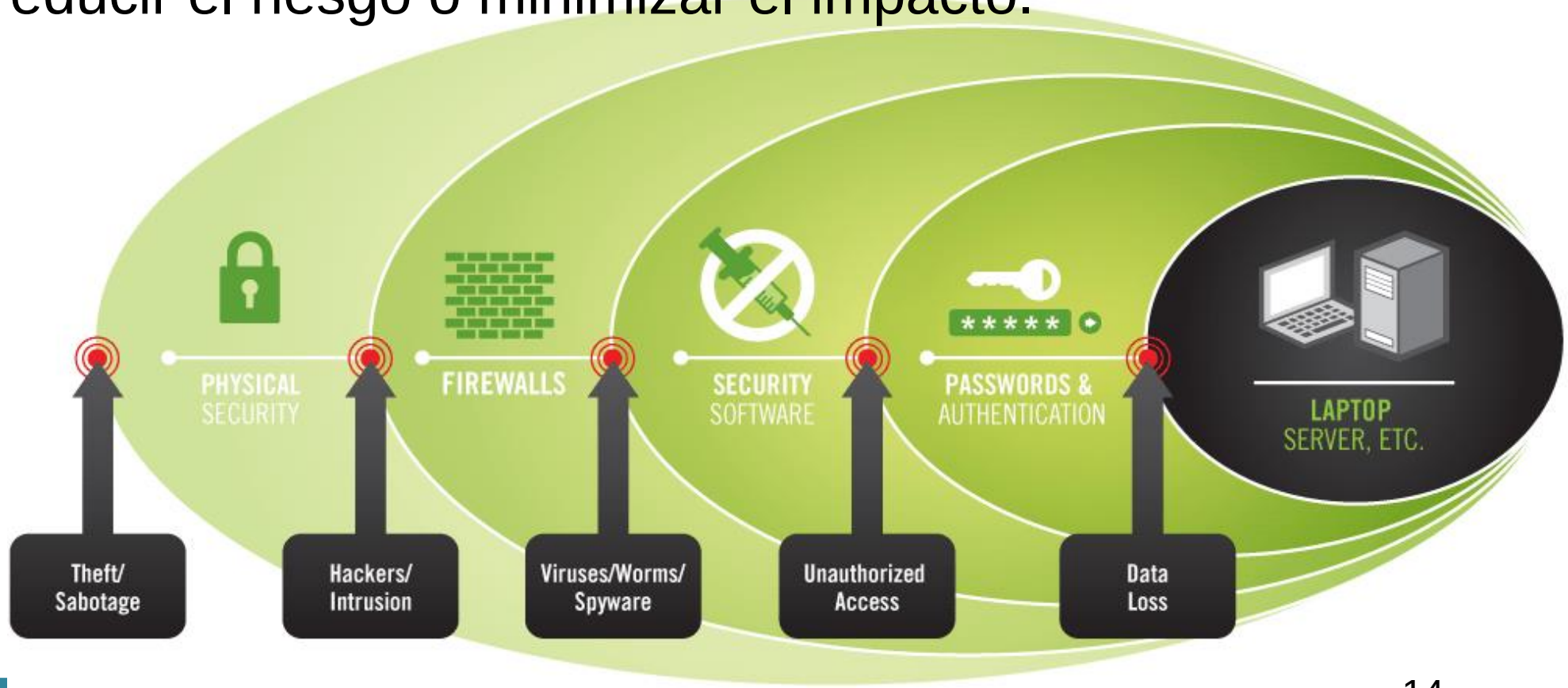
- NECESIDAD-DE-CONOCER
  - Los usuarios solo deben tener acceso a la información (a los sistemas) que necesiten para realizar sus funciones.
  - También se referencia como **Principio de MÍNIMO PRIVILEGIO**
  - Relacionado con el **Principio de SEPARACIÓN DE FUNCIONES** (roles): repartir las responsabilidades.



13

Principio de la defensa en profundidad

- Estrategia de protección con múltiples capas de seguridad para reducir el riesgo o minimizar el impacto.



14

Gestionar la seguridad

- **Una seguridad organizada**
  - SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información.
  - ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System
- **Concienciación**
- **Implementaciones**

Avanzando hacia el análisis de seguridad

- Activos
- Amenazas
- Vulnerabilidades
- Incidentes de seguridad
- Impactos
- Riesgos
- Defensas, salvaguardas o medidas de seguridad
- Transferencia del riesgo a terceros

16

BIBLIOGRAFÍA

00	**Cano, J. et al., "Regulación y ciberseguridad: Contribuciones al modelo de Gobernanza". https://www.researchgate.net/publication/283641837_Regulacion_y_ciberseguridad_Contribuciones_al_modelo_de_Gobernanza**		
01	Recomendación UIT-T X.1205: Aspectos generales de la cibersecuridad. http://www.itu.int/rec/T-REC-X.1205-200804-I	66	pdf
02	Theoharidou, M.; Gritzalis, D., "Common Body of Knowledge for Information Security," *Security & Privacy, IEEE* , vol.5, no.2, pp.64,67, March-April 2007 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4140992&isnumber=4140976	4	pdf
03	ISO/IEC 27000		web
04a	Avizienis, A.; Laprie, J.-C.; Randell, B.; Landwehr, C., "Basic concepts and taxonomy of dependable and secure computing," Dependable and Secure Computing, IEEE Transactions on , vol.1, no.1, pp.11,33, Jan.-March 2004	23	

AMPLIACIÓN

#	Material	pp	tipo
01	CyberCIEGE security video game. http://www.cisr.us/cyberciege		web
02	CyberProtect security exercise game. http://iase.disa.mil/eta/cyber-protect/launchcontent.html		web
03	Karl D. Stephan, Katina Michael, M.G. Michael, Laura Jacob, and Emily Anesta. "Social Implications of Technology: Past, Present, and Future" *Proceedings of the IEEE* 100.13 (2012): 1752-1781. Available at: http://works.bepress.com/kmichael/255	30	doc
04	JinKyu Lee; Bagchi-Sen, S.; Rao, H.R.; Upadhyaya, S.J., "Anatomy of the Information Security Workforce," *IT Professional* , vol.12, no.1, pp.14,23, Jan.-Feb. 2010	10	doc
05	Ed Crowley. 2003. Information system security curricula development. In Proceedings of the 4th conference on Information technology curriculum (CITC4 '03). ACM, New York, NY, USA, 249-255.	7	doc
06	Open Security Training. Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK) Review. Information Security & Risk Management Domain. http://opensecuritytraining.info		web
07	Glosario de términos de seguridad en Internet. RFC 4949. http://tools.ietf.org/html/rfc4949		web
08	Guía de seguridad de las TIC (CCN-STIC-401). Glosario y abreviaturas. https://www.ccn-cert.cni.es/publico/serieCCN-STIC401		web

ACADEMIA DE INGENIEROS

SEMINARIO SOBRE LOS PRINCIPIOS BÁSICOS DE LA CIBERSEGURIDAD

Estado de alarma, 12 de mayo de 2020