DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Introducción – Clase 2

Fundamentos de ciberseguridad

Profesor
Juan Ignacio Iturbe A.

Objetivos de aprendizaje

- OA5: Explicar y definir los conceptos básicos de la ciberseguridad.

Definiciones

- Ciberseguridad

"Condición de estar **protegido** en contra de consecuencias físicas, sociales, espirituales, financieras, emocionales, ocupacionales, psicológicas, educacionales o de otro tipo que resultan del fallo, daño, error, accidentes perjuicios o cualquier otro evento en el **Ciberespacio** que se pueda considerar no deseable"

ISO 27032 (2015) Tecnologías de la información – Técnicas de seguridad – Directrices para la ciberprotección

Definiciones

- Ciberseguridad

"El proceso de **proteger** la información mediante la prevención, detección y respuesta a los ataques"

Framework for Improving Critical Infrastructure Cybersecurity, NIST (2018).

Definiciones

- Ciberespacio

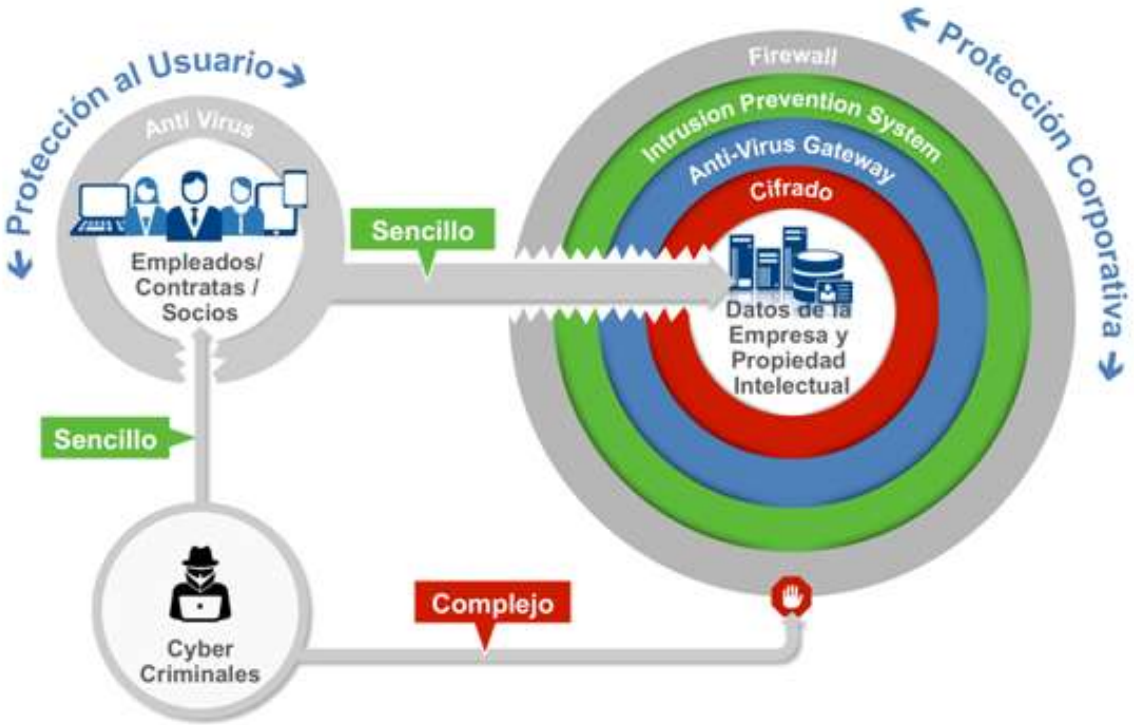
  "Entorno complejo que resulta de la interacción de personas, softwares y servicios en Internet por medio de dispositivos y redes de tecnología conectados a éste, los que no existen en forma física"

ISO 27032 (2015) Tecnologías de la información – Técnicas de seguridad – Directrices para la ciberprotección

Definiciones

- Cibercrimen

  “Actividad criminal que implica que los servicios o aplicaciones en el Ciberespacio se utilicen o sean blanco de un crimen, lo que significa que e Ciberespacio es la fuente, herramienta, blanco o lugar de un crimen”



https://www.ibm.com/blogs/think/es-es/2015/02/24/cuidado-con-las-apts/

Definición

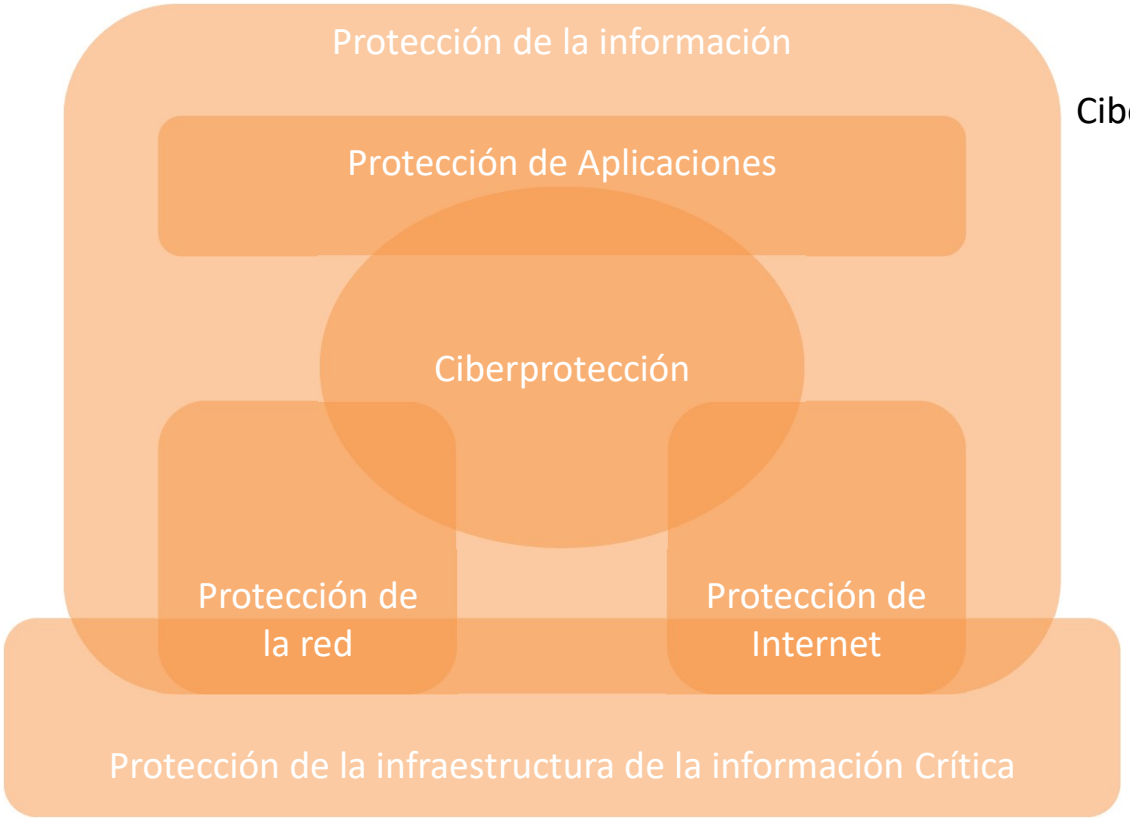
- Ciberprotección

  “Conservación de la **confidencialidad**, **integridad** y **disponibilidad** de la información en el ciberespacio”

ISO 27032 (2015) Tecnologías de la información – Técnicas de seguridad – Directrices para la ciberprotección

Relación entre los conceptos

Cibercrimen



Ciberseguridad

ISO 27032 (2015) Tecnologías de la información – Técnicas de seguridad – Directrices para la Ciberprotección

Principios de Seguridad

- Tenemos que entender los objetivos principales de la seguridad:
  - *–disponibilidad, integridad y confidencialidad*
- Los cuales deben dar protección a los **activos críticos e información.**

Principios de Seguridad

- **Disponibilidad:** es la protección que asegura confiabilidad y acceso oportuno a los datos y recursos para individuos autorizados.

(Suena mas fácil de lo que es)
¿Ejemplos que afecten la disponibilidad?

Principios de Seguridad

- **Integridad:** se cumple cuando se proporciona garantía de la exactitud y fiabilidad a la información y sistemas. Cualquier modificación no autorizada se evita.
    - Por ej:
        - Cuando un atacante inserta un virus, una bomba lógica o un *back door* en el sistema, la integridad del mismo se ve comprometida.
        - Cuando un usuario tiene acceso full al disco duro, puede creer que borrar el boot.ini está bien, ya que no recuerda haberlo utilizado.
        - ¿otros ejemplos?

Principios de Seguridad

- **Confidencialidad:** asegura que el nivel necesario de secreto se aplica en cada cruce de procesamiento de datos y se evita la divulgación no autorizada.
  - Esto se debe aplicar desde el emisor de los datos, en dispositivos de la red que es transmitida y una vez que llegue a su destino.

Por ej, comprometen este principio: ingeniería social y *shoulder surfing*.

Resumen

- Se desarrolló un ejercicio sobre los conceptos básicos de ciberseguridad en el cual a partir del conocimiento del estudiante se resolvió.
- Luego se discutió a nivel de curso y se volvió a revisar las preguntas a nivel grupal.
- Se revisaron algunos de estos conceptos con definiciones formales.
- Se resolvieron dudas sobre los conceptos.

Recursos bibliográficos

- https://www.ciberseguridad.gob.cl/
- Biblioteca digital USACH – AENOR
- ISO/IEC 27K
- https://www.incibe.es/