DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Introducción

Conceptos generales y objetivos de la ciberseguridad

Profesor

Juan Ignacio Iturbe A.

Resultado de aprendizaje de la sesión

“Explicar y definir los conceptos básicos de la ciberseguridad aplicándolos a situaciones reales”

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

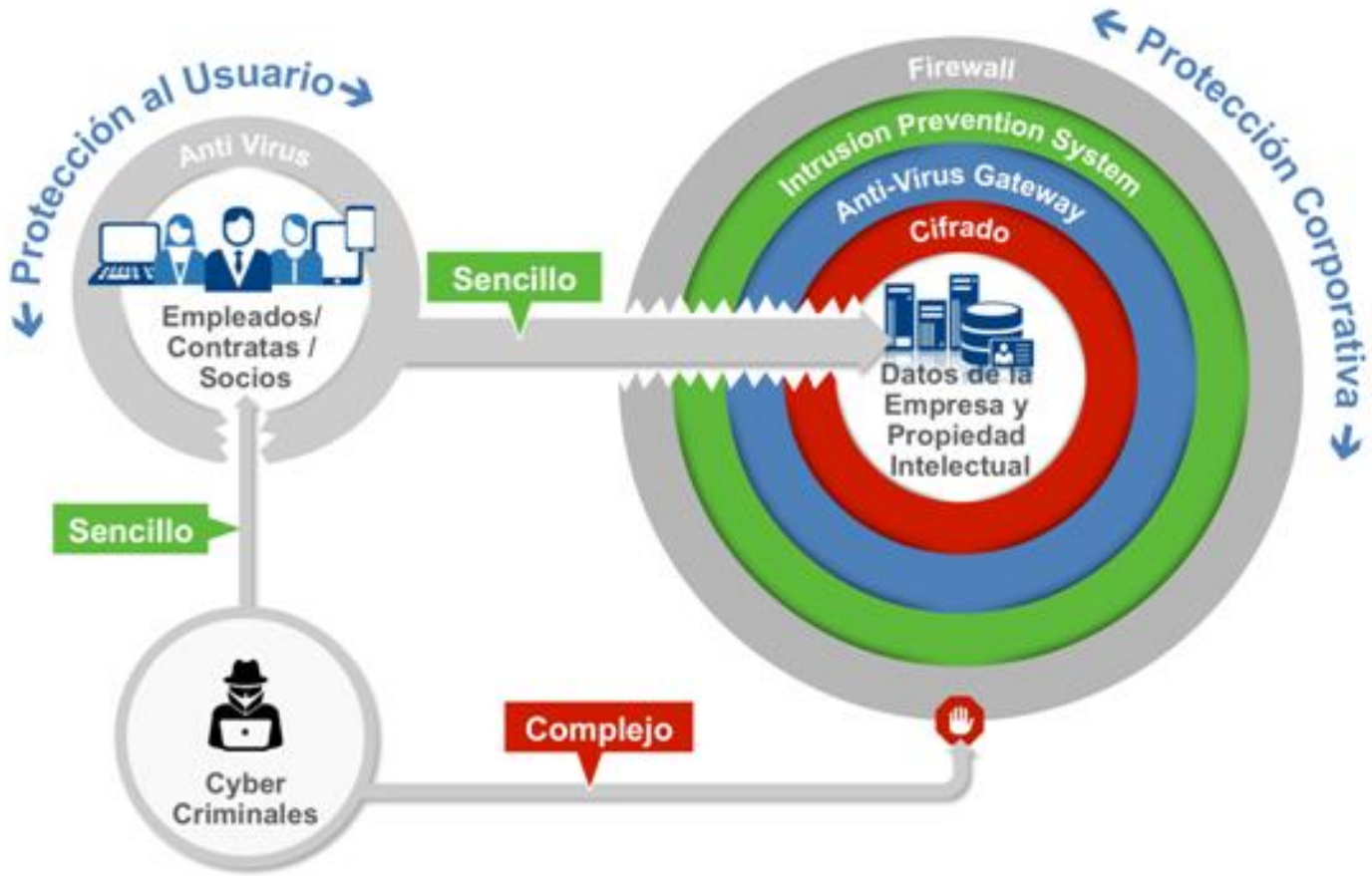
  “Entorno complejo que resulta de la interacción de personas, softwares y servicios en Internet por medio de dispositivos y redes de tecnología conectados a éste, los que no existen en forma física”

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

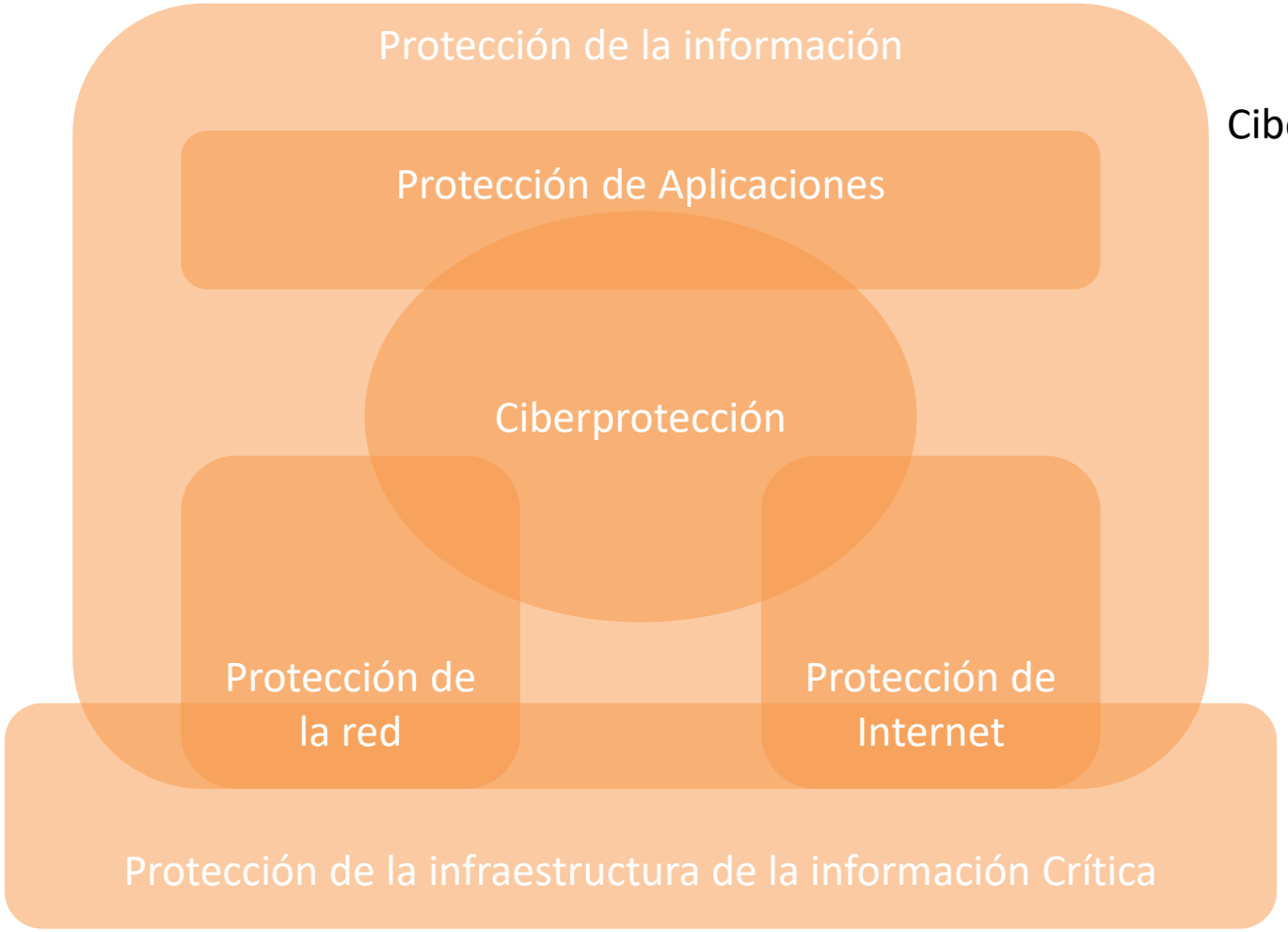
- Ciberprotección

"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

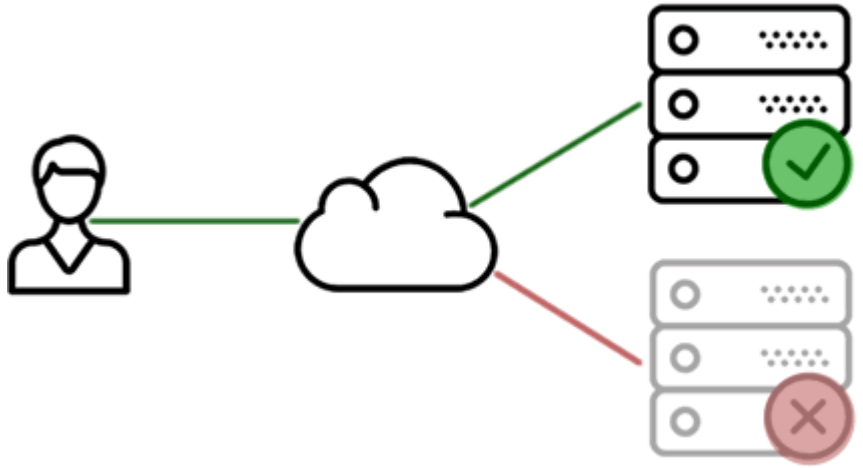
Objetivos de la ciberseguridad

- Disponibilidad (*Availability*)
- Integridad (*Integrity*)
- Confidencialidad (*Confidentiality*)
- Autenticidad (*Authenticity*)
- No repudio (*Non-repudiation*)
- Rendición de cuentas (*Accountability*)

Objetivos de la ciberseguridad

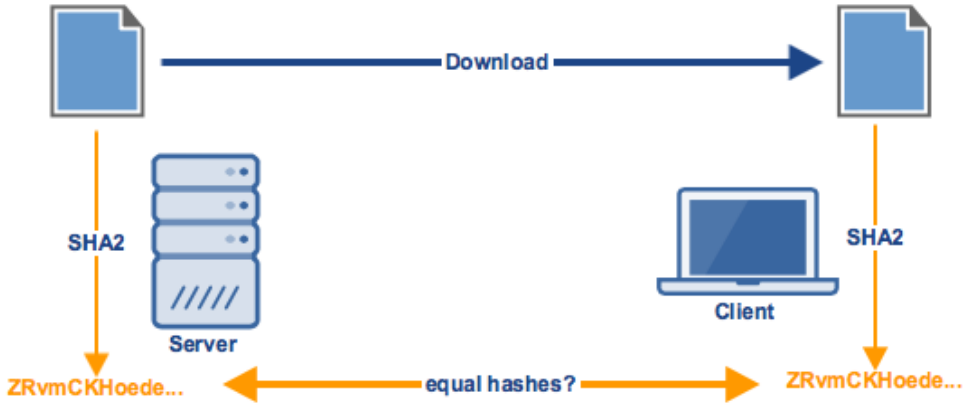
- **Disponibilidad:** es la protección que asegura confiabilidad y acceso oportuno a los datos y recursos para individuos autorizados.
  - Por ej:
    - Las redes tienen muchas piezas que deben estar disponibles al mismo tiempo (servidores DNS, DHCP, routers, switches, proxies, firewalls)
    - El software tiene muchas piezas que deben funcionar en conjunto de forma sana (SO, aplicaciones, antimalware).

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



Objetivos de la ciberseguridad

- **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?



Objetivos de la ciberseguridad

Confidencialidad:

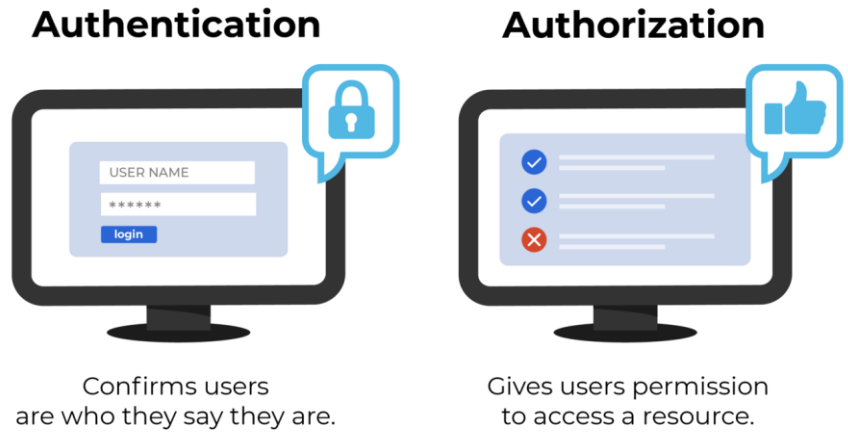
- Asegura que el nivel necesario de secreto se aplica en cada cruce de procesamiento de datos y se evita la divulgación no autorizada.
  - Esto se debe aplicar desde el emisor de los datos, en dispositivos de la red que es transmitida y una vez que llegue a su destino.

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

Objetivos de la ciberseguridad

Autenticidad

- La propiedad de ser genuino y poder ser verificado y confiable.
- Esto significa verificar que los usuarios son quienes dicen ser y que cada entrada que llega al sistema proviene de una fuente confiable.



Objetivos de la ciberseguridad

No repudio

- Garantía de que el remitente de la información es provisto con una prueba de entrega y el destinatario recibe la prueba de la identidad del remitente en un punto específico de tiempo
- Ninguno de los dos puede negar más tarde haber procesado la información.
  - Ej. El correo que indica la realización de una transacción bancaria.

Objetivos de la ciberseguridad

Rendición de cuentas

- La propiedad de un sistema o recurso del sistema que garantiza que las acciones de una entidad del sistema puedan rastrearse de forma exclusiva a esa entidad,
- Esta entidad luego puede ser considerada responsable de sus acciones.

Actividad formativa individual: ¿A que objetivo de la ciberseguridad se relacionan los siguientes ejemplos?

- Hashing
- Redundant array of independent disk (RAID) Gestión de la configuración
- Funciones de rollback
- Control de cambios
- Clustering
- Encriptación para data en reposo (todo el disco, de base de datos)
- Control de acceso
- Ingeniería social
- Propiedad del protocolo TLS para asegurar que un sitio es quien dice ser
- Respaldo de software y datos
- Encriptación de datos en transito (IPSec, TLS, PPTP, SSH)
- Firma digital de software
- Autenticación en dos pasos
- Logs de auditoria
- Balanceo de cargas
- Grabación telefónica de una transacción
- Funciones CRC para la transmisión
- Shoulder surfing
- Líneas de energía y datos redundantes

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/