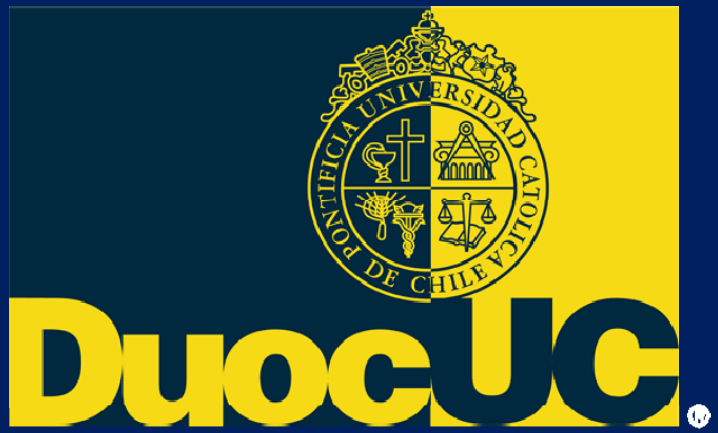


Semana 1: Control de Acceso

Seguridad Informática

Aprendizajes esperados

Contenidos:

- Principios de Seguridad Informática
- Triada de la Seguridad Informática
- Servicios de Seguridad
- Técnicas de identificación y autenticación

Principios de Seguridad Informática

- Como consecuencia de la amplia difusión de la tecnología informática, la información:
  - Se almacena y procesa en computadores, que pueden ser independientes o estar conectados a sistemas de redes.
  - Puede ser confidencial para algunas personas o para instituciones completas.

Principios de Seguridad Informática

- Puede utilizarse para fines poco éticos.
- Puede divulgarse sin autorización de su propietario.
- Puede estar sujeta a robos, sabotaje o fraudes.
- Puede ser alterada, destruida y mal utilizada.

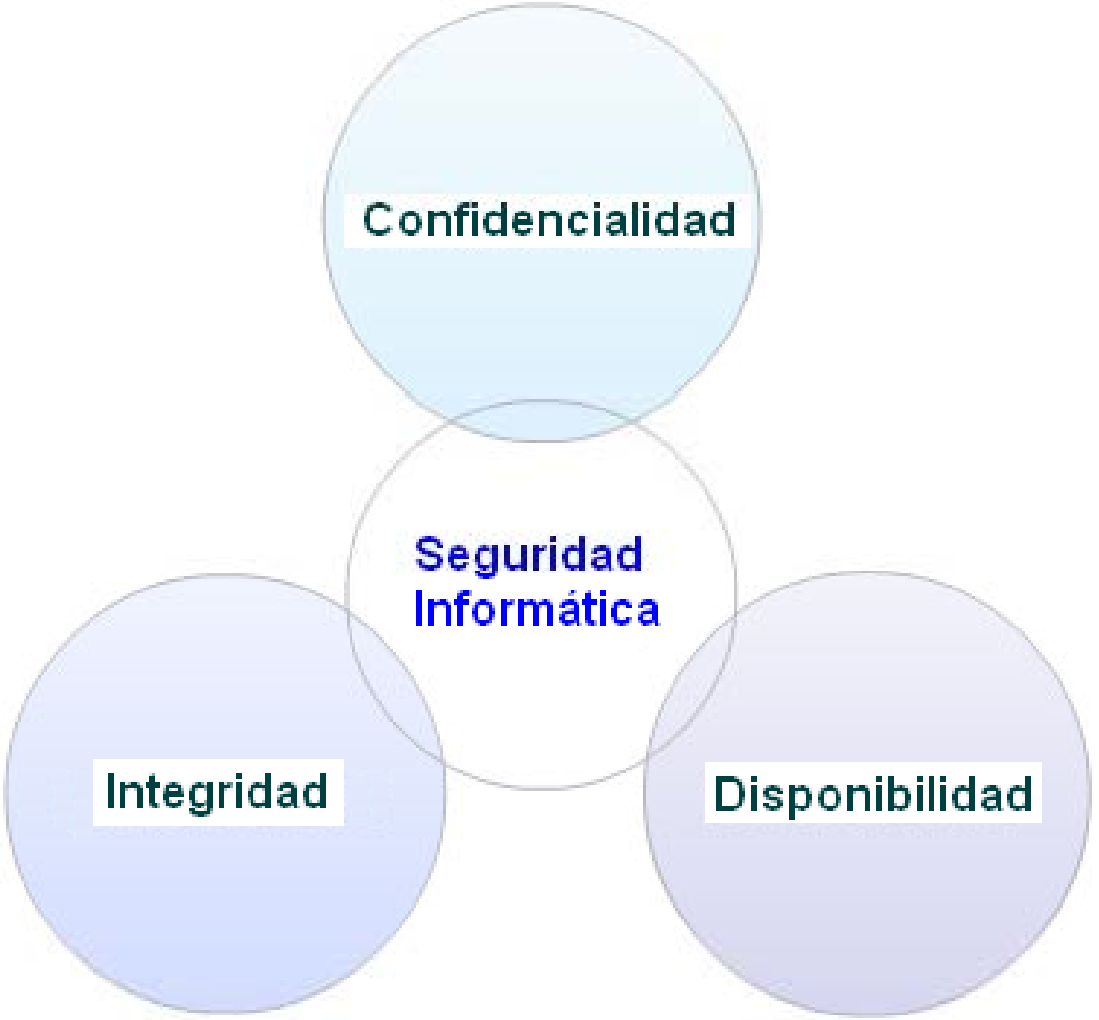
Principios de Seguridad Informática

- La **SEGURIDAD INFORMÁTICA** es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.
- La decisión de aplicarlos es responsabilidad de cada usuario.

Triada de la Seguridad Informática

- Para lograr sus objetivos, la **SEGURIDAD INFORMÁTICA** se fundamenta en tres principios, que debe cumplir todo sistema informático:
  - **CONFIDENCIALIDAD**
  - **INTEGRIDAD**
  - **DISPONIBILIDAD**

Triada de la Seguridad Informática



Triada de la Seguridad Informática

- La **CONFIDENCIALIDAD** se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático.
- Basándose en este principio, las herramientas de seguridad informática deben proteger al sistema de invasiones, intrusiones y accesos, por parte de personas o programas no autorizados.

Triada de la Seguridad Informática

- Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los que usuarios, computadores y datos residen en localidades diferentes, pero están física y lógicamente interconectados.

Triada de la Seguridad Informática

- La **INTEGRIDAD** se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático.
- Este principio es particularmente importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios, computadores y procesos comparten la misma información.

Triada de la Seguridad Informática

- Basándose en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos.

Triada de la Seguridad Informática

- Este principio es particularmente importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios, computadores y procesos comparten la misma información.

Triada de la Seguridad Informática

- La **DISPONIBILIDAD** se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático.
- Este principio es particularmente importante en sistemas informáticos cuyo compromiso con el usuario, es prestar servicio permanente.

Triada de la Seguridad Informática

- Basándose en este principio, las herramientas de Seguridad Informática deben reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran.

Servicios de Seguridad

- El objetivo de un **SERVICIO DE SEGURIDAD** es mejorar la seguridad de los sistemas de procesamiento de datos y la transferencia de información en las organizaciones. Los **SERVICIOS DE SEGURIDAD** están diseñados para contrarrestar los ataques a la seguridad y hacen uso de uno o más mecanismos de seguridad para proporcionar el servicio.

Servicios de Seguridad

- El **NO REPUDIO** proporciona protección contra la interrupción, por parte de alguna de las entidades implicadas en la comunicación, de haber participado en toda o parte de la comunicación.
- El servicio de Seguridad de **NO REPUDIO** o irrenunciabilidad está estandarizado en la ISO-7498-2.

Servicios de Seguridad

- **NO REPUDIO DE ORIGEN**: El emisor no puede negar que envío porque el destinatario tiene pruebas del envío, el receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor, de negar tal envío, tenga éxito ante el juicio de terceros. En este caso la prueba la crea el propio emisor y la recibe el destinatario.

Servicios de Seguridad

- El **NO REPUDIO DE ORIGEN** prueba que el mensaje fue enviado por la parte específica.

Servicios de Seguridad

- **NO REPUDIO DE DESTINO**: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. Este servicio proporciona al emisor la prueba de que el destinatario legítimo de un envío, realmente lo recibió, evitando que el receptor lo niegue posteriormente.

Servicios de Seguridad

- En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.
- El **NO REPUDIO DE DESTINO** prueba que el mensaje fue recibido por la parte específica.

Servicios de Seguridad

- Si la **AUTENTICIDAD** prueba quién es el autor de un documento y cual es su destinatario, el "**NO REPUDIO**" prueba que el autor envió la comunicación (**NO REPUDIO EN ORIGEN**) y que el destinatario la recibió (**NO REPUDIO EN DESTINO**).

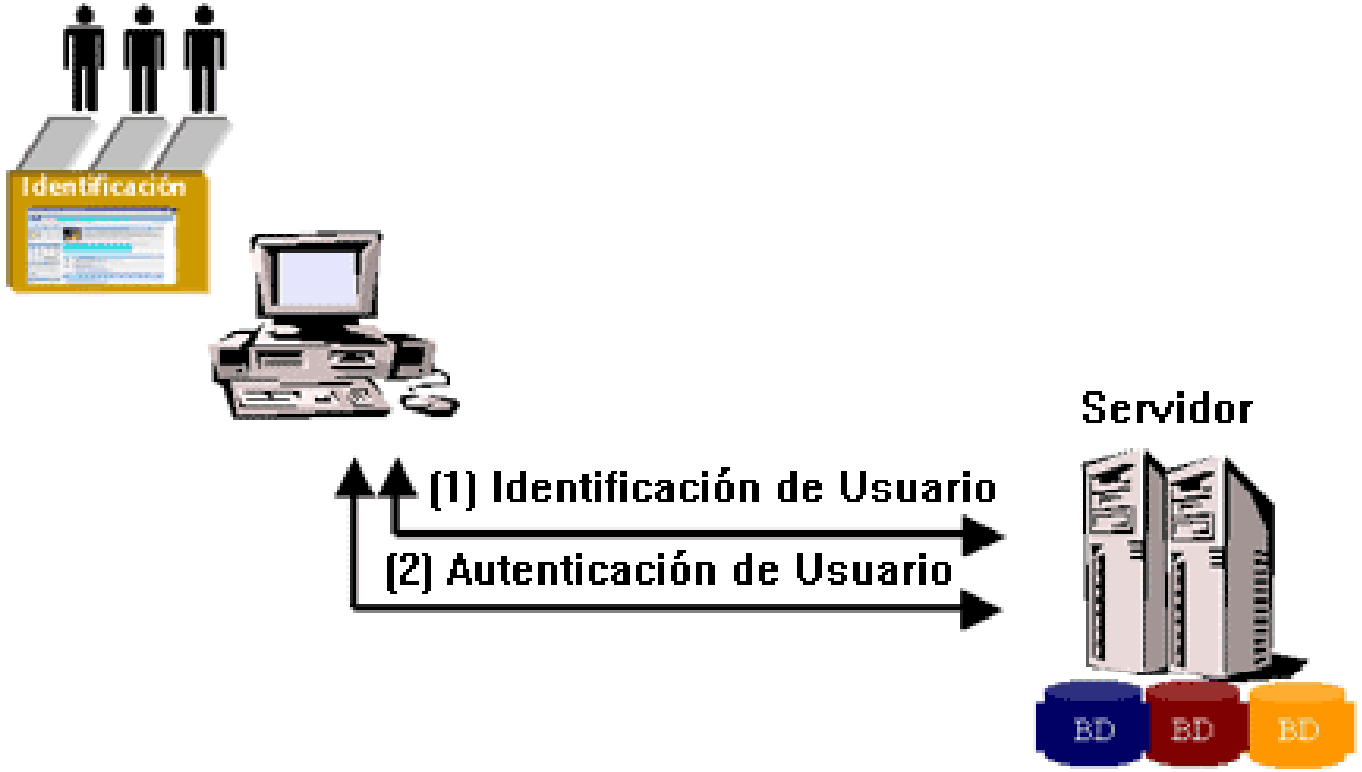
Técnicas de Identificación y Autenticación

- El proceso de **IDENTIFICACIÓN** y **AUTENTICACIÓN** corresponde a la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas.
- Es la base para la mayor parte de los **CONTROLES DE ACCESO** y para el seguimiento de las actividades de los usuarios.

Técnicas de Identificación y Autenticación

- Se denomina **IDENTIFICACIÓN** al momento en que el usuario se da a conocer en el sistema; y **AUTENTICACIÓN** a la verificación que realiza el sistema sobre esta identificación.

Técnicas de Identificación y Autenticación



Técnicas de Identificación y Autenticación

- Al igual que se consideró para la **SEGURIDAD FÍSICA**, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

Técnicas de Identificación y Autenticación

- **Algo que solamente el individuo conoce**: por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc.
- **Algo que la persona posee**: por ejemplo una tarjeta magnética.

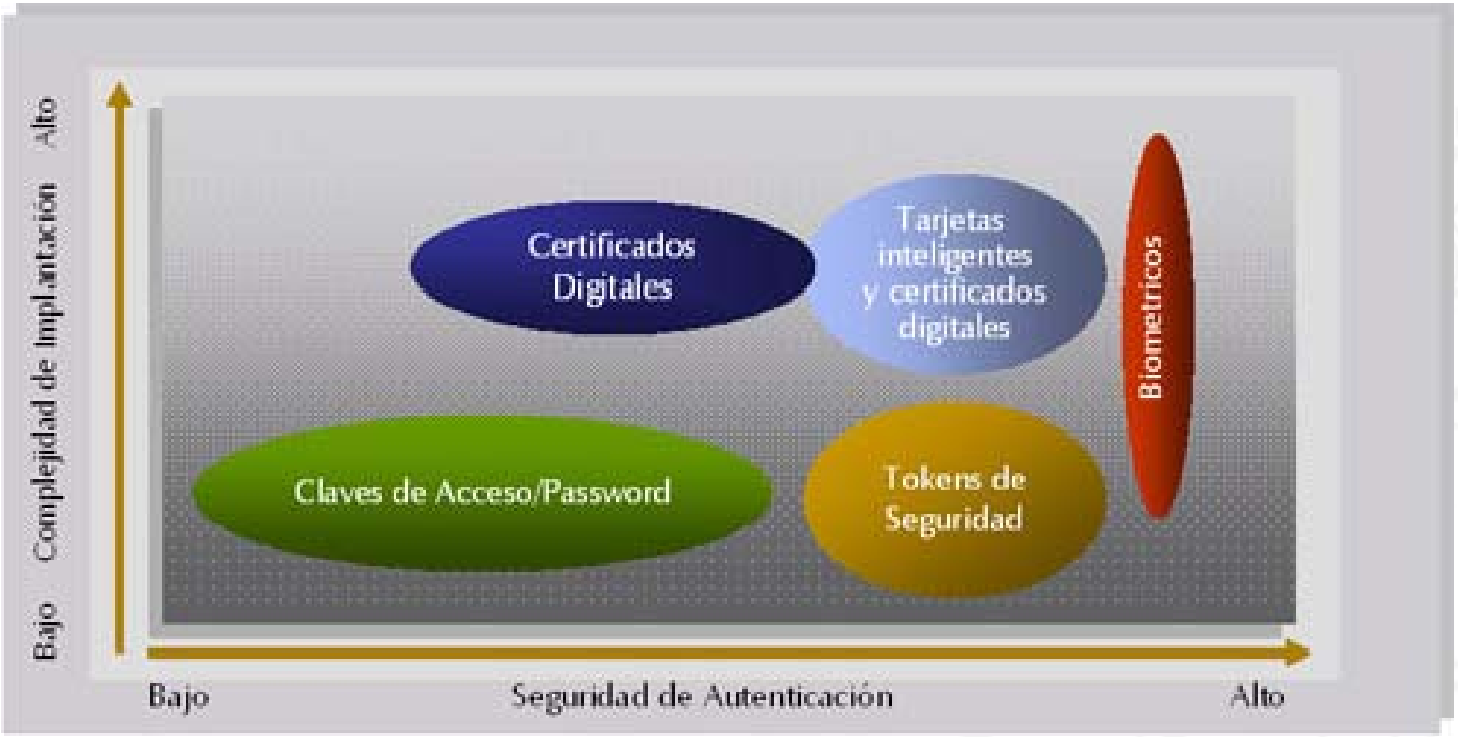
Técnicas de Identificación y Autenticación

- **Algo que el individuo es y que lo identifica unívocamente**: por ejemplo las huellas digitales o la voz.
- **Algo que el individuo es capaz de hacer:** por ejemplo los patrones de escritura.

Técnicas de Identificación y Autenticación

- En la siguiente figura, se muestran las diferentes tecnologías que apoyan el mecanismo de **AUTENTICACIÓN** de usuarios y su relación con la complejidad de implantación.

Técnicas de Identificación y Autenticación



Técnicas de Identificación y Autenticación

- Para cada una de estas técnicas vale lo mencionado en el caso de la **SEGURIDAD FÍSICA** en cuanto a sus ventajas y desventajas.
- Se destaca que en los dos primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan.

Técnicas de Identificación y Autenticación

- Mientras que por otro lado, los controles de autenticación biométricos serían los más apropiados y fáciles de administrar, resultando ser también, los más costosos por lo dificultoso de su implementación eficiente.

Técnicas de Identificación y Autenticación

- Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de allí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota.

Técnicas de Identificación y Autenticación

- Esto se denomina "single login" o sincronización de passwords.
- Una de las posibles técnicas para implementar esta única identificación de usuarios sería la utilización de un **SERVIDOR DE AUTENTICACIONES** sobre el cual los usuarios se identifican, y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder.

Técnicas de Identificación y Autenticación

- La **SEGURIDAD INFORMÁTICA** se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos.

Resumen

- La **INFORMACIÓN** puede ser divulgada, mal utilizada, ser robada, borrada o saboteada.
- Esto puede afectar su disponibilidad y la pone en riesgo.
- La **SEGURIDAD DE LA INFORMACIÓN** tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.

Resumen

- Las técnicas o métodos que se utilizan para tener una correcta organización de seguridad para la información están basadas en los pilares que ofrece la **TRIADA DE LA SEGURIDAD**: confidencialidad, integridad y disponibilidad.