

Seguridad, privacidad y aspectos legales

Introducción a la seguridad de la información

Álvaro López García

Grupo de Computación Avanzada y e-Ciencia
Instituto de Física de Cantabria (IFCA) - CSIC-UC

Máster universitario en ciencia de datos / Master in Data Science



CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS

CSIC



Parte I


Introducción a la seguridad de la información

1. Conceptos Generales

Conceptos Generales

Definición

Medidas preventivas y reactivas de las personas, organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información manteniendo íntegras sus propiedades de seguridad (como confidencialidad, disponibilidad e integridad).



- Protección de los activos en un sistema informático.
- Activos: información (datos, en nuestro caso). 
- Tipos de protección:
 - Prevención: tomar medidas para preservar la seguridad.
 - Detección: detectar cuando, cómo y quién ha roto la seguridad de un activo.
 - Reacción: mitigar y reparar los daños causados.
- Propiedades de seguridad de los activos: **confidencialidad**, **autenticidad**, trazabilidad, anonimización, **integridad**, **no repudia**, disponibilidad.

Confidencialidad

Prevención de la difusión no autorizada (no divulgación) de la información (secreto).

Privacidad

Derecho a no ser objeto de intrusión de terceros (privado).

- Conceptos relacionados pero no similares.
- Se puede preservar una pero no la otra.
- Ejemplo: una empresa cede de forma consciente datos de sus usuarios a un tercero, sin nuestro consentimiento.
 - Se preserva la confidencialidad entre las empresas. 
 - No se conserva la privacidad.
- Métodos: autenticación y autorización, cifrado, control de acceso. 
- Definir quién puede acceder a y/o modificar qué.
- Conceptos relacionados: Anonimización.

Definición

Identificación y garantía del origen de la información.

- Asegurar que quién origina la información es quien realmente dice ser.
- Evitar la suplantación de la identidad.
- Relacionado con la integridad.




Definición

No alteración, manipulación, modificación o corrupción (intencional o no) de la información cuando es manejada (transmitida, almacenada, procesada, etc.) por un sistema de información.

- Asegura que la información sea correcta y sin errores.
- Asegura que la información no pueda ser modificada sin permiso
- Asegurar la corrección e invarianza de la información. Confiabilidad
- Método: hash.
- Ejemplo: paquetes linux

Definición

Guardar trazas de todas las acciones susceptibles de comprometer la seguridad de un sistema, para asegurar que se puede identificar al culpable o implicado.

- Es imposible prevenir frente a todo tipo de acciones.
 - Acciones autorizadas pueden violar la seguridad (error de diseño).
 - Acciones no autorizadas.
- El sistema debe guardar trazas de todas las acciones: traza de auditoría.
- Prerequisitos: identificación de usuarios.
- Quién hizo qué.

Definición

Delimitar y suprimir la información concreta que permite identificar a los individuos concretos.

- Anonimato, pseudoanonimato (reversible), anonimato.
- Relacionado con privacidad y confidencialidad.
- Conflicto con autenticidad, trazabilidad y no-repudio



Definición

Proveer evidencia de que un evento específico ha ocurrido.

- Comprobar la identidad del emisor de un mensaje.
- Evitar que alguna de las partes de una comunicación niegue una acción.
- Métodos: firmas digitales. Servicios de no repudia de entrega (e.g. burofax).

Definición

Asegurar que la información está accesible cuando se requiera acceder a ella.

- Prevenir que un atacante impida el acceso a los activos de forma legítima.
- Métodos: redundancia de disco, servidores, localidad, backups.

Ejemplos: Seguridad en un hospital

- Integridad: asegurar que el tratamiento es el adecuado.
- Confidencialidad: prevenir que los datos de los pacientes se hagan públicos.
- Privacidad: asegurar que solo el personal habilitado puede acceder al historial de un paciente.
- Imposibilidad de usar registros anónimos.
- Consentimiento informado: ¿qué se puede hacer con mis datos?

Ejemplos: Seguridad en un entorno científico

- Integridad y trazabilidad: asegurar que los datos de los experimentos son correctos y no son manipulados (datos primarios, secundarios, terciarios).
- Confidencialidad: prevenir que los datos se hagan públicos antes de que finalice un embargo.
- Seguridad en el acceso.
- Disponibilidad.

- La seguridad se puede ver comprometida aunque tomemos medidas para protegerla, por ejemplo: la anonimización puede no ser suficiente.
- Ejemplo: Resonancias magnéticas del cráneo pueden ser suficientes para identificar a una persona.
- Ejemplo: Publicación de delitos anonimizados, con data aggregation para obtener información de la persona.

Ejemplos: Autenticidad e integridad

- En 2008 un atacante consiguió romper la seguridad de las distribuciones Fedora y RedHat.
 - Se firmaron paquetes falsos como legítimos (OpenSSH).
 - Esto puede comprometer la seguridad de cientos de miles de servidores.
 - <https://lwn.net/Articles/295406/>
- En 2010 un atacante consiguió acceder a varios servidores de <https://kernel.org>.
 - La integridad del kernel no estuvo en riesgo, pero hubo un problema de reputación.
 - <https://pastebin.com/BKcmMd47>

Preguntas?