CAPITULO 1
Nociones de Seguridad de la Información
Conceptos de Seguridad de la Información según ISO 27001

Jenny Torres, PhD.

Propiedades de la Seguridad

CIA

- No existe un sistema 100 % seguro, pero se debe intentar dar un nivel tolerable de seguridad a los usuarios.
- Para que un sistema sea razonable o tolerablemente seguro, este debe cumplir al menos con tres propiedades de la seguridad:
  - Confidencialidad
  - Integridad
  - Disponibilidad

CIA

Confidencialidad

- *"Propiedad de que la información no esté disponible o no sea divulgada a personas, entidades o procesos no autorizados".*

- Se trata básicamente de la propiedad por la que esa información solo resultará accesible con la debida y comprobada autorización.

- ¿Cómo se pierde esa confidencialidad? Generalmente, haciendo caso omiso a las recomendaciones de seguridad o no implantando un sistema adecuado; así, cuando compartimos equipos sin eliminar las contraseñas, olvidamos cerrar nuestro usuario, tiramos un disco duro sin borrar antes sus datos o no ciframos los datos de manera adecuada, la información deja de ser confidencial y entramos, digamos, en una zona de alto riesgo.

CIA

Integridad

- *"Propiedad de proteger la precisión y completitud de los activos"*
- La integridad hace referencia a la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros.
- Esta integridad se pierde cuando la información se modifica o cuando parte de ella se elimina, y una gran garantía para mantenerla intacta es, como hemos mencionado en anteriores ocasiones, la firma digital.
- Un aspecto relacionado con la integridad es la autentificación, cualidad que permite identificar al generador de la información y que se logra con los correctos accesos de usuario y con otros sistemas como la recientemente mencionada firma electrónica. Para algunos, incluso, la autentificación sería el "cuarto pilar" de la Seguridad de la Información.

CIA

Disponibilidad

- *“Propiedad de estar disponible y utilizable en el momento en que sea requerido por una entidad autorizada”.*
- Por disponible entendemos aquella información a la que podemos acceder cuando la necesitamos a través de los canales adecuados siguiendo los procesos correctos.
- Esta característica, la disponibilidad, puede en ocasiones chocar frontalmente con la confidencialidad, ya que un cifrado complejo o un sistema de archivado más estricto puede convertir la información en algo poco accesible, por lo que no se trata en absoluto de un punto menor y marca en gran medida el buen hacer del responsable de la seguridad de la información de la empresa u organización.

Otras características de la seguridad

- **Autenticidad**: Propiedad de que una entidad es lo que expresa ser. El origen de un mensaje ha de ser perfectamente identificado.
  - **Autenticación**: Característica o propiedad de la seguridad que garantiza que lo que una entidad afirma ser es correcta.
  - **Autorización**: Característica o propiedad de la seguridad relacionada con el control de acceso.
  - **No repudio**: Capacidad de probar la ocurrencia de un evento. Ni el emisor del mensaje, ni el receptor del mismo pueden negar que se haya efectuado el mismo.

Otras características de la seguridad

- **Accountability** (Rendición de Cuentas): Se refiere al registro de acciones en la empresa para garantizar la no repudiación (en transacciones), disuasión, aislamiento de fallas, detección y prevención de intrusiones, recuperación y toma de acciones legales.
  - Asociada a la auditoría y a la computación forense.
  - Se demanda la capacidad de asociar una brecha de seguridad con el responsable, para obtener evidencia.

Términos y Definiciones relacionados con la Seguridad

- **Vulnerabilidad**
  - Debilidad de un activo o control.
  - Se define como la susceptibilidad de algo para absorber negativamente incidencias externas.
  - Es una vía de ataque potencial.

- **Amenaza**
  - Causa potencial de un evento no deseado, el cual puede resultar en daños al activo o a la organización.
  - Es una acción o evento que puede violar la seguridad de un entorno de Sistemas de Información.
  - Tiene tres componentes:
    - *Objetivo*: El aspecto de la seguridad que puede ser atacado.
    - *Agente*: Las personas u organizaciones que originan la amenaza.
    - *Evento*: El tipo de acción que origina la amenaza.

Términos y Definiciones relacionados con la Seguridad

- **Riesgo**
  - Posibilidad de que una amenaza explote una vulnerabilidad de un activo o grupo de activos, que cause daños a la organización.
  - Probabilidad de que la amenaza actúe sobre el activo. Se utiliza para cuantificar el daño (probable) que puede causar la amenaza.
  - Amenaza + Vulnerabilidad = Riesgo

- **Activo de Información**
  - Conocimiento, datos (información) que tienen valor para la organización.

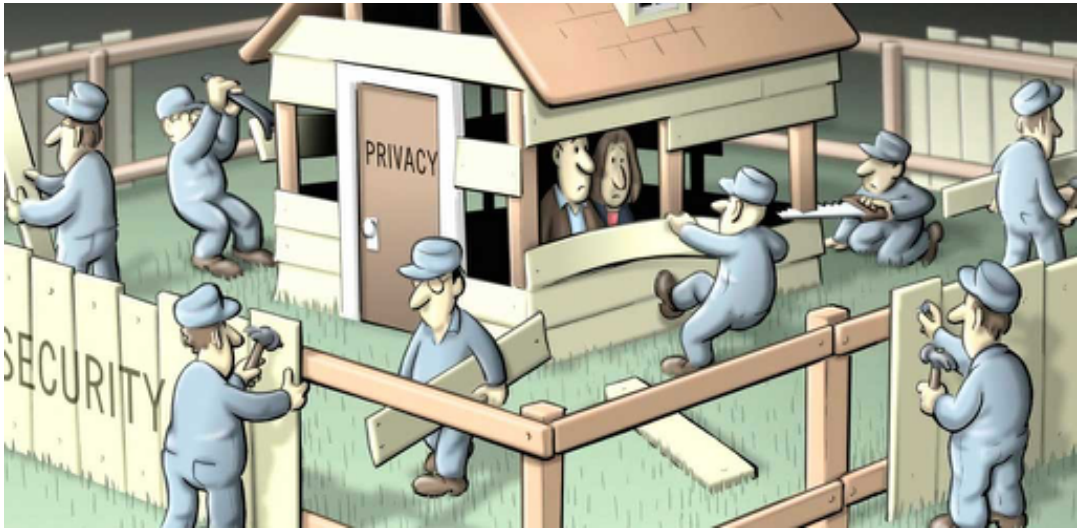
- **Ataque**
  - Intento de destruir, exponer, alterar, desactivar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.

Términos y Definiciones relacionados con la Seguridad

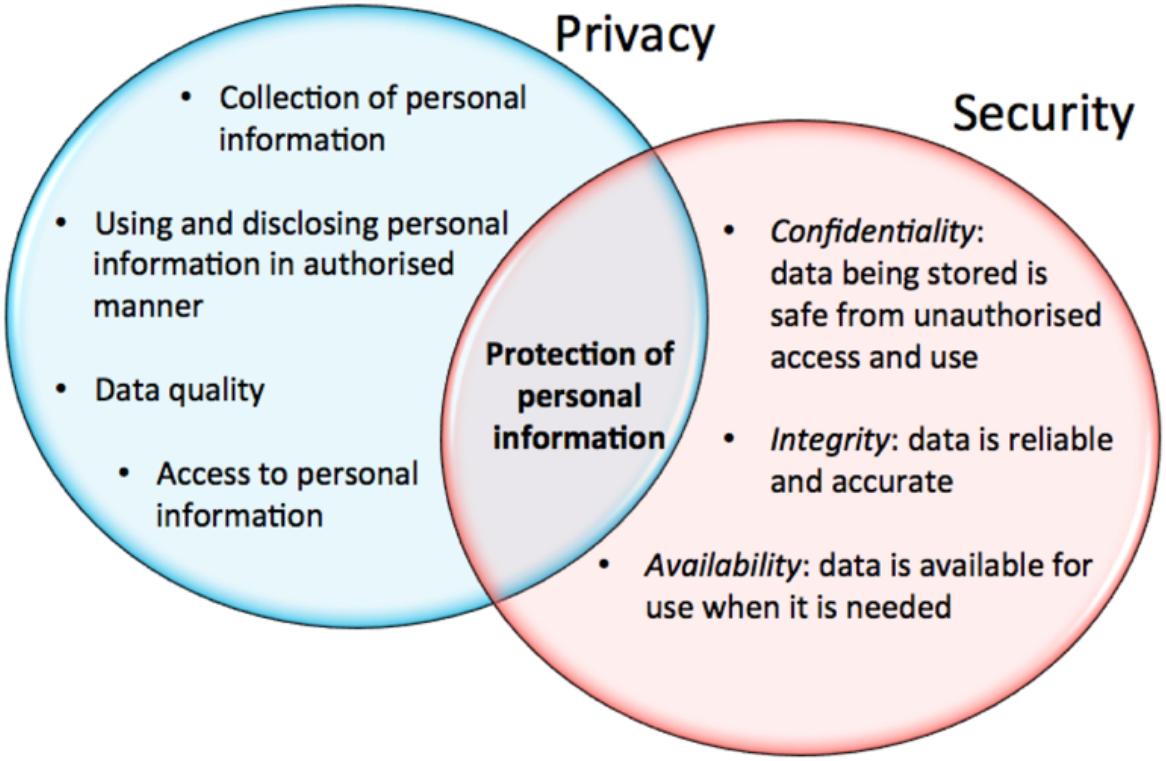
- **Evento de Seguridad**
  - Ocurrencia identificada de una condición de un sistema, servicio o red que indica una posible violación de la poĺ ıtica, falla en controles o una situación previamente desconocida.
- **Incidente**
  - Evento o serie de eventos no deseados o inesperados con gran probabilidad de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Impacto**
  - Cambio adverso al nivel alcanzado de los objetivos del negocio. Ej. El efecto que un evento inesperado puede causar sobre los activos.

Seguridad vs. Privacidad

- **Seguridad**: Preservación de las características CIA de la información.
- **Privacidad**: Propiedad de preservación de una persona, entidad o proceso para evitar revelarse o revelar información relacionada ellos mismo.



Seguridad vs. Privacidad



Referencias

- INEN (2012) Descripción General y Vocabulario. Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27000:2012.

- Stallings, W. (2011) Network Security Essentials 4th edition, New York, US; ISBN:13: 978-1587052460: Prentice-Hall.