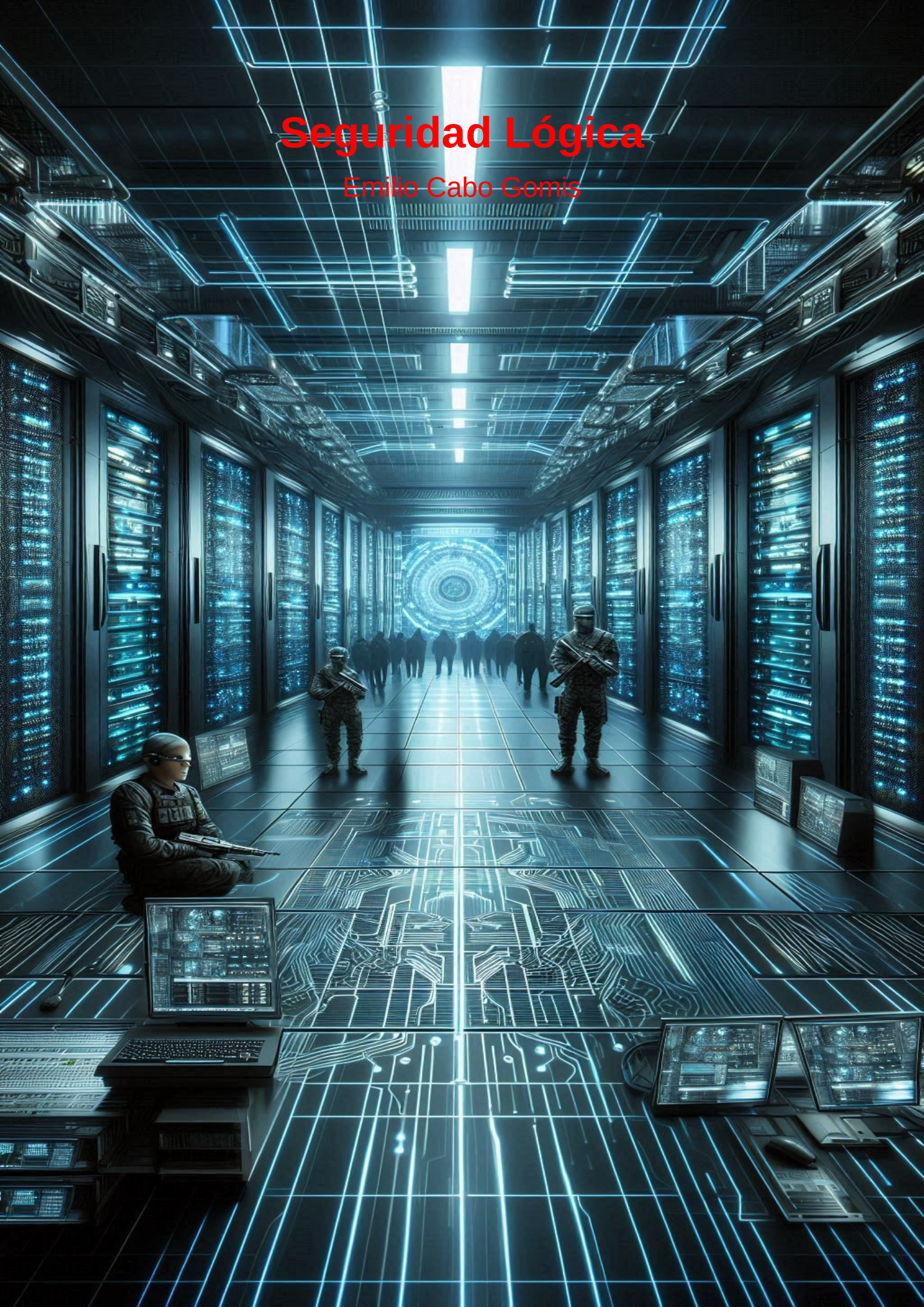


Seguridad Lógica

Emilio Cabo Gomis

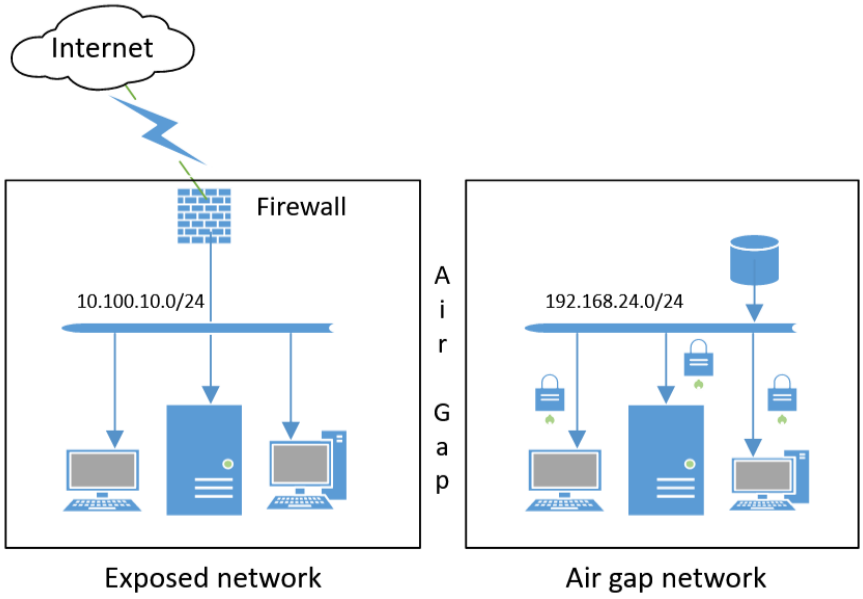
Sumario

¿Cuales son las bases de la Seguridad Informática?

Fiabilidad

La fiabilidad en referencia a la seguridad de un sistema informático se refiere a la probabilidad de que un sistema funcione según lo esperado. Para que un sistema sea considerado fiable, debe cumplir con tres aspectos fundamentales:

- **Confidencialidad**: Garantizar que la información no sea divulgada a personas no autorizadas.
- **Integridad**: La integridad de la información se refiere ala exactitud, coherencia y confiabilidad de la información. Las medidas de integridad protegen la información de alteraciones no autorizadas. Estas medidas garantizan la exactitud e integridad de los datos.
- **Disponibilidad**: Prevenir interrupciones no autorizadas o no controladas de los recursos informáticos. La disponibilidad de la información puede verse interrumpida por actores maliciosos. Ataques de Denegación de servicios, DNS, ARP pueden ser utilizados para explotar vulnerabilidades del sistema.



Hay posiblemente una relación inversa entre lo accesible que es un sistema informático y lo seguro que es. Aunque nunca podemos decir que un sistema informático es del todo seguro. *"El único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de concreto, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aún así, yo no apostaría mi vida por él" (Eugene Spafford).*

Si que podemos decir que es un sistema bastante seguro.

Por ejemplo si encripto el disco con el sistema operativo de mi ordenador, olvido la clave y lo desconecto de la red. Es un sistema súper seguro pero es inusable. Debemos poder usar el sistema y acceder a el. Lo que lo hace inherentemente inseguro

Autenticación y control de acceso

La autenticación y el control de acceso que permite verificar la identidad de quien accede a un recurso y se le permite o no el acceso según dicha identidad.

Control de acceso: Se refiere a la gestión de los permisos que determinan qué acciones puede realizar un usuario una vez autenticado.

Métodos de Autenticación:

Algo que el usuario Posee: Tarjetas RFID, Chips NFC

Algo que el usuario sabe: Preguntas de seguridad, contraseñas, pin

Algo que el usuario es: Acceso biométrico.

Es importante implementar métodos de control de acceso para la información, permisos, usuarios, autenticación, autorización.

Una ocurrencia muy común son las filtraciones.
Enviar un archivo “Confidencial” en un email sin querer como archivo adjunto, filtraciones en redes sociales.
Esta filtración podría haberse evitado de tener las medidas adecuadas de autorización y autenticación. Cómo podría ser haber configurado los permisos de acceso o copiado de los archivos, directamente en Windows o mediante una herramienta de terceros.

CIDAN

Los cinco objetivos de la seguridad:

1. **Confidencialidad**: Protege la información para que solo las personas autorizadas puedan acceder a ella.
2. **Integridad**: Garantiza que la información no se ha alterado de manera no autorizada.
3. **Disponibilidad**: Asegura que la información y los sistemas estén disponibles cuando se necesiten.
4. **Autenticación**: Verifica la identidad de las personas que acceden a los sistemas.

5. **No repudio**: Asegura que ninguna de las partes pueda negar su participación en una comunicación.