# Clase 1:
# Conceptos básicos de ciberseguridad

# Triada de la ciberseguridad

## CIA

**Confidencialidad (confidentiality):** mantener la información exclusiva de sus dueños.

**Integridad (integrity):** mantener la información igual que cuando fue creada.

**Disponibilidad (availability):** mantener la información disponible para sus dueños siempre que la necesiten.

# Triada de la ciberseguridad – Confidencialidad

## Contraseñas

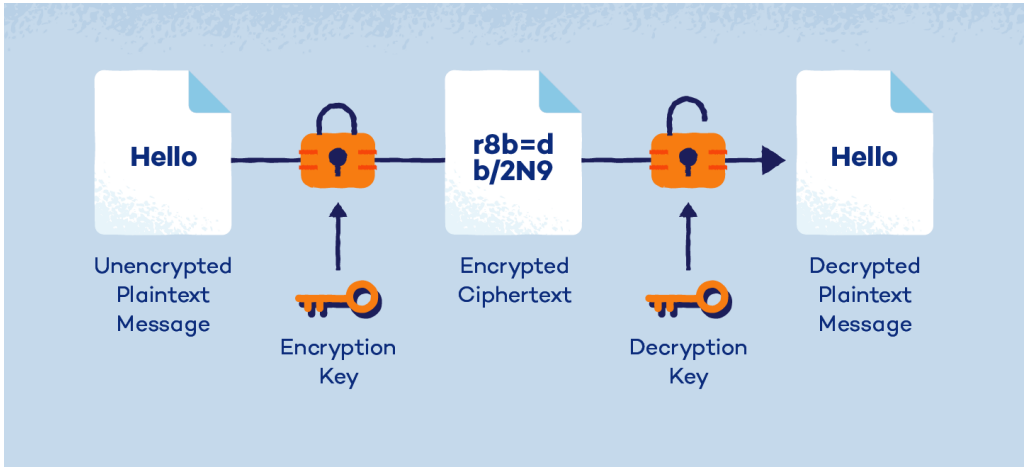
**Knowledge based factors**

- Credentials stored on a server
- SMS OTP
- Security questions
- Passwords

**Possession and inherence based factors**

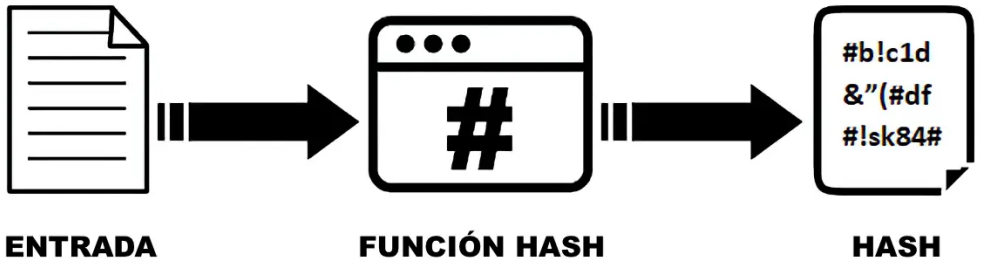
- Credentials on-device (never on a server)
- Local Biometric / PIN
- Multi-device FIDO credentials (Passkeys)

## Encriptación

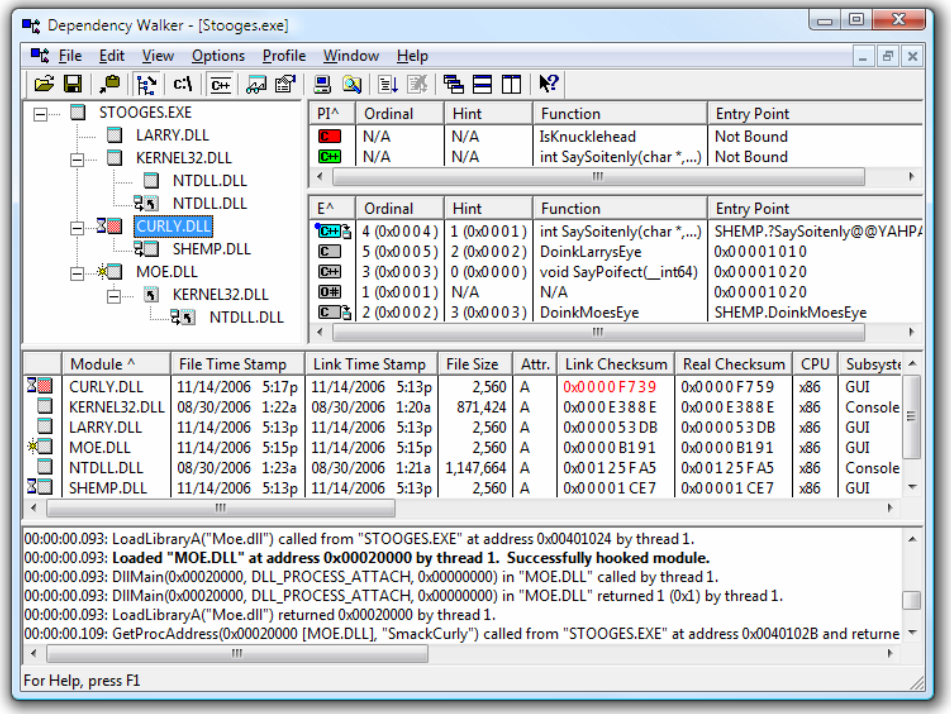


# Triada de la ciberseguridad – Integridad

## Hashes

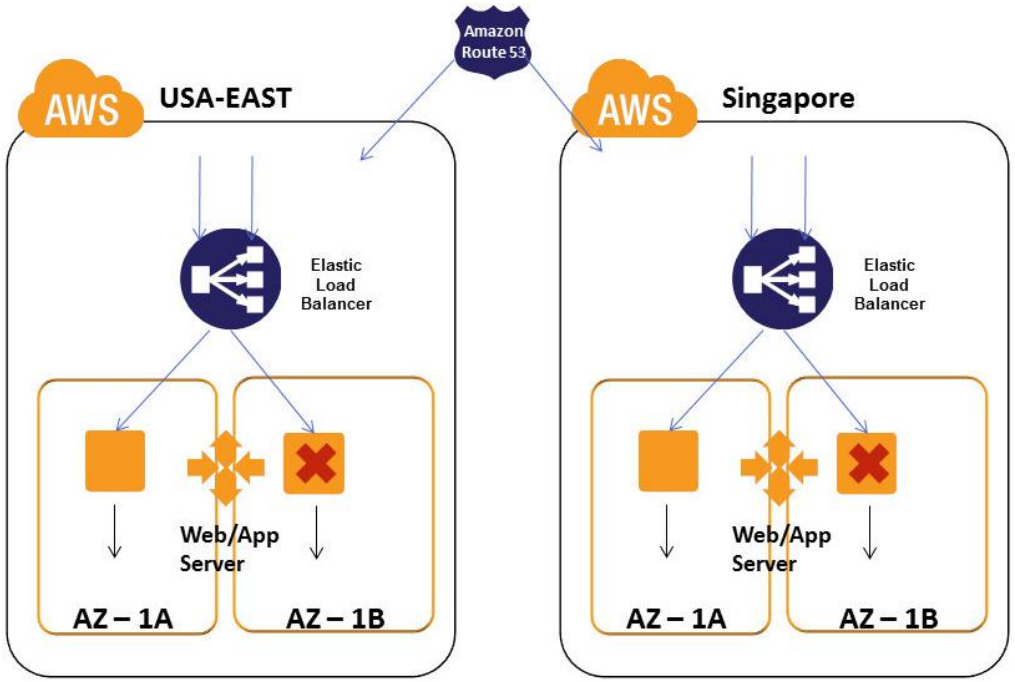



## Captura de DLLs



# Triada de la ciberseguridad – Disponibilidad

## Redundancia de datos




## ISPs alternos



ISP = Internet Service Provider (Proveedor de Servicios de Internet)

# Control de entendimiento

¿Cuáles son los conceptos conocidos como “la triada de ciberseguridad”?

Confidencialidad, Integridad y Disponibilidad

# Controles de seguridad – Cateogorías

## Categorías de controles

- Control técnico: ejecutados por sistemas técnicos (control de acceso, encriptación...).
- Control gerencial/administrativo: procesos y procedimientos organizacionales de seguridad (revisión de bagage, campañas de concientización...); usualmente controlados y difundidos por personas.
- Control operacional: incluyen cultura organizacional y controles físicos contra acceso directo a datos (respaldos, control de disponsitivos, diseño de puertas, cerraduras...).
- Control físico: proveen seguridad a la ubicación física (sensores de movimiento/fuego/agua, cámaras, cerraduras, sistemas biométricos...).

# Controles de seguridad – Tipos según su función

## Tipos de controles según su función

- Control preventivo: intentan prevenir eventos inesperados inhabilitando uso libre de recursos computacionales (control de acceso, IPS, DLP, firewalls, antivirus...).
- Control disuasorio (para asustar): buscan desanimar a individuos de violar políticas y procedimientos de seguridad; no necesariamente detienen acceso no autorizado (señalización, avisos, cámaras, agentes de seguridad...).
- Control correctivo: son reactivos y proveen medidas para reducir daños o restaurar sistemas (actualizaciones de sistemas, restauración de repaldos, mitigación de vulnerabilidades...).
- Control compensatorio: entran en juego cuando existen restricciones ante otros controles (ser cuidadoso en lugar de comprar antivirus, usar sistema alternativo si uno no soporta contraseñas fuertes...).

# Controles de seguridad – Tipos según su función

## Tipos de controles según su función

- Control directivo: similares a los disuasorios, pero centrados en enseñar qué hacer para prevenir o alertar de eventos de seguridad (campañas contra phishing, políticas y procedimientos...).

# Control de entendimiento

¿Qué tipo(s) y categoría es el control mostrado en la imagen?


Categoría: física; Tipo: disuasorio

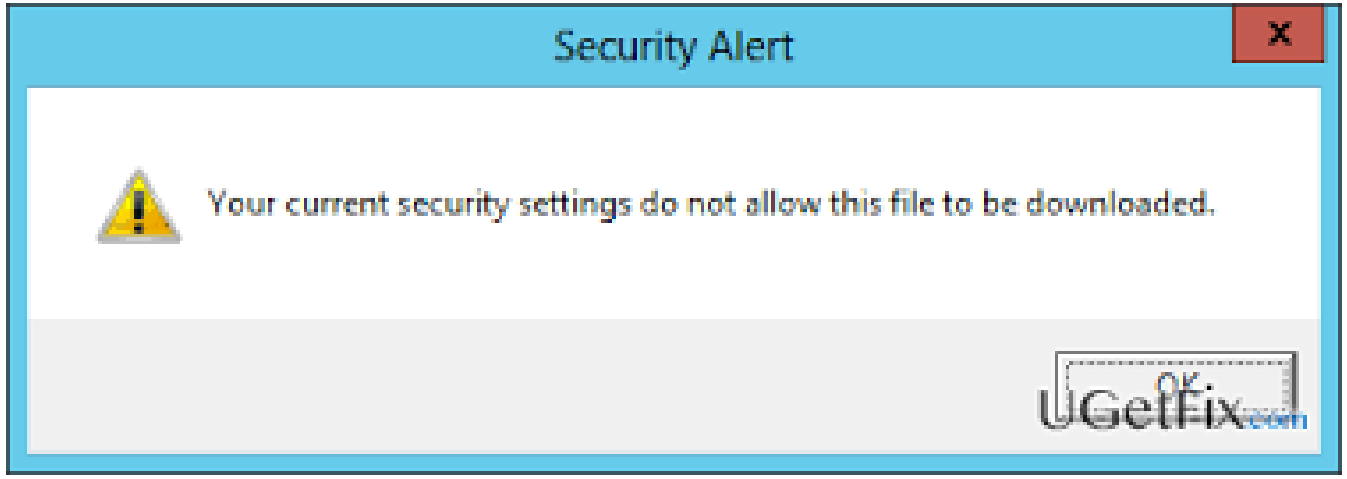
# Control de entendimiento

## ¿Qué tipo(s) y categoría es el control mostrado en la imagen?

Categoría: físico; Tipo: disuasorio, preventivo, correctivo

# Control de entendimiento

## ¿Qué tipo(s) y categoría es el control mostrado en la imagen?




Categoría: técnico; Tipo: preventivo

# Marco de trabajo AAA

AAA es un marco de trabajo (framework) que controla el uso de recursos computacionales, refuerzan políticas y audita su uso.

**Autenticación (authentication)**: quién tiene acceso.

**Autorización (authorization)**: a qué se tiene acceso.

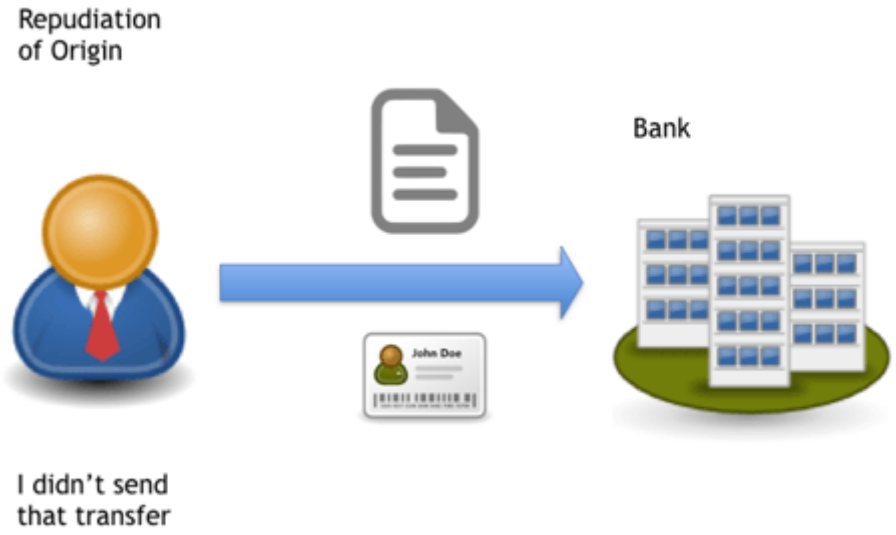
**Registro (accounting)**: qué fue accedido.


Va de la mano con la triada CIA

# Principio de no repudio (non-repudiation)

Es un principio de seguridad que se asegura de que los actores no puedan negar/repudiar sus acciones y transacciones realizadas. El objetivo es brindar pruebas para comprobar las acciones y transacciones.

Ejemplo:
Un sistema informático que tiene varios usuarios y un registro de logs puede demostrar que cierto usuario realizó la modificación de una factura para reflejar menos dinero del movido, y tomar ese dinero.



# Control de entendimiento

¿Qué conceptos componen el framework AAA?

Autenticación, Autorización y Registro

# Control de entendimiento

¿El principio de no repudio busca proveer confianza en una red informática ?

Falso:

Provee pruebas para que un actor no pueda negar que realizó una acción/transacción.