

Clase 1: Conceptos básicos de ciberseguridad



Triada de la ciberseguridad

CIA

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

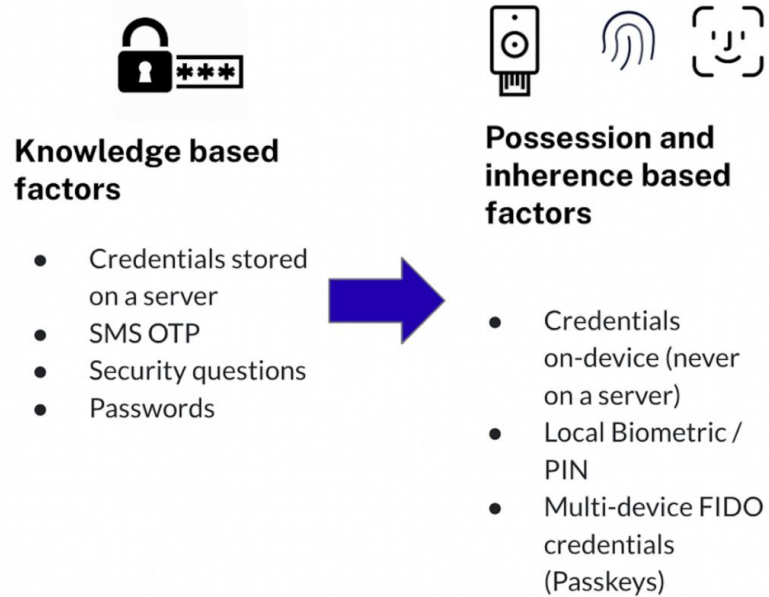
Integridad (integrity): mantener la información igual que cuando fue creada.

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

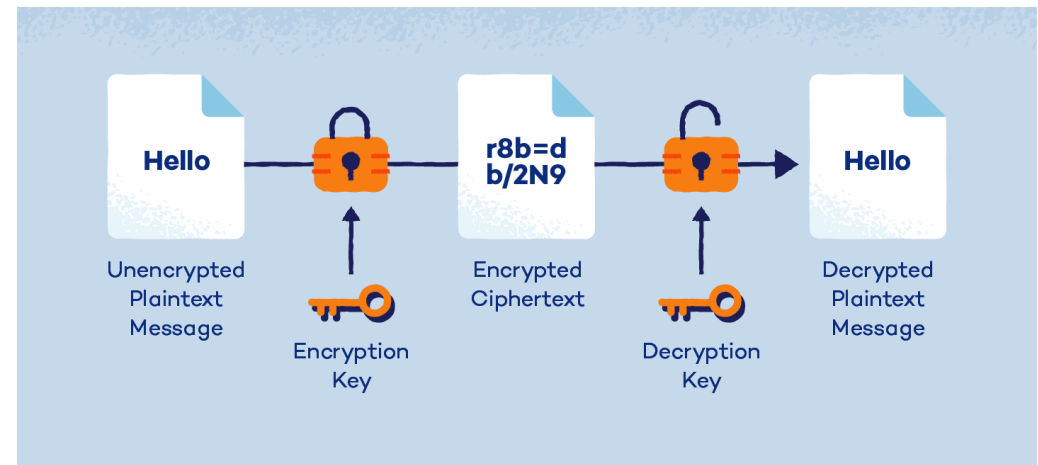


Triada de la ciberseguridad – **Confidencialidad**

Contraseñas

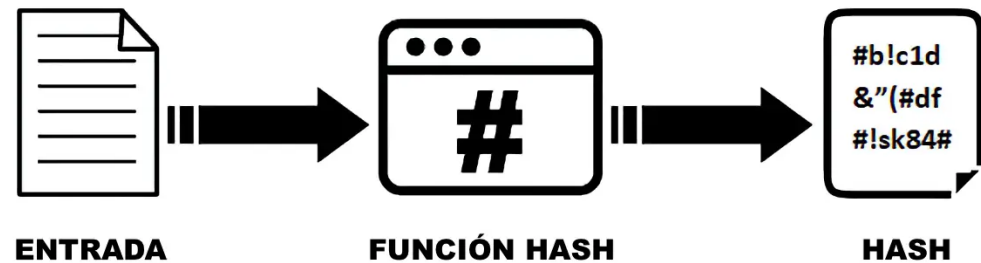


Encriptación



Triada de la ciberseguridad – Integridad

Hashes



Captura de DLLs

The screenshot shows the Dependency Walker window for 'Stooges.exe'. The left pane lists loaded modules, including CURLY.DLL, LARRY.DLL, MOE.DLL, and SHEMP.DLL. The right pane shows the function list for the selected module (CURLY.DLL). The bottom pane shows the call stack, including the 'LoadLibraryA' function call for 'Moe.dll'.

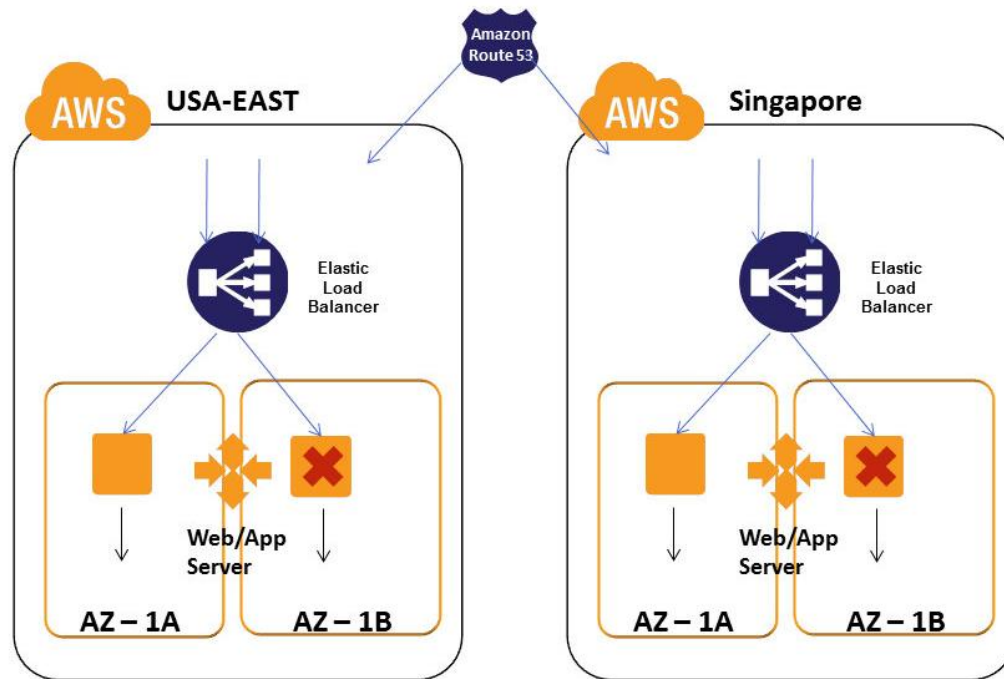
Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem
CURLY.DLL	11/14/2006 5:17p	11/14/2006 5:13p	2,560	A	0x0000F739	0x0000F759	x86	GUI
KERNEL32.DLL	08/30/2006 1:22a	08/30/2006 1:20a	871,424	A	0x000E388E	0x000E388E	x86	Console
LARRY.DLL	11/14/2006 5:13p	11/14/2006 5:13p	2,560	A	0x000053DB	0x000053DB	x86	GUI
MOE.DLL	11/14/2006 5:15p	11/14/2006 5:15p	2,560	A	0x0000B191	0x0000B191	x86	GUI
NTDLL.DLL	08/30/2006 1:23a	08/30/2006 1:21a	1,147,664	A	0x00125FA5	0x00125FA5	x86	Console
SHEMP.DLL	11/14/2006 5:13p	11/14/2006 5:13p	2,560	A	0x00001CE7	0x00001CE7	x86	GUI

Call Stack (bottom):

- 00:00:00.093: LoadLibraryA("Moe.dll") called from "Stooges.exe" at address 0x00401024 by thread 1.
- 00:00:00.093: Loaded "MOE.DLL" at address 0x00020000 by thread 1. Successfully hooked module.
- 00:00:00.093: DllMain(0x00020000, DLL_PROCESS_ATTACH, 0x00000000) in "MOE.DLL" called by thread 1.
- 00:00:00.093: DllMain(0x00020000, DLL_PROCESS_ATTACH, 0x00000000) in "MOE.DLL" returned 1 (0x1) by thread 1.
- 00:00:00.093: LoadLibraryA("Moe.dll") returned 0x00020000 by thread 1.
- 00:00:00.109: GetProcAddress(0x00020000 [MOE.DLL], "SmackCurly") called from "Stooges.exe" at address 0x0040102B and returned...

Triada de la ciberseguridad – Disponibilidad

Redundancia de datos



ISPs alternos

¡Internet eres tú!

CONÉCTATE CON
Fibra Óptica
150 MEGAS
CON Claro-tv+
POR \$45 AL MES

tigo

Adquirí tu **PLAN HOGAR**

Hasta **120 Mbps** x \$41.99 /mes
+ TV Digital HD

1 MES DE CORTESÍA | **VIX Premium**

TIGUENIALS

Solicítalo al **8888-0999**
o marcá ***611**

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

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

Confidencialidad, Integridad y Disponibilidad

Controles de seguridad – Categorías

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 dispositivos, 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: físico; Tipo: disuasorio

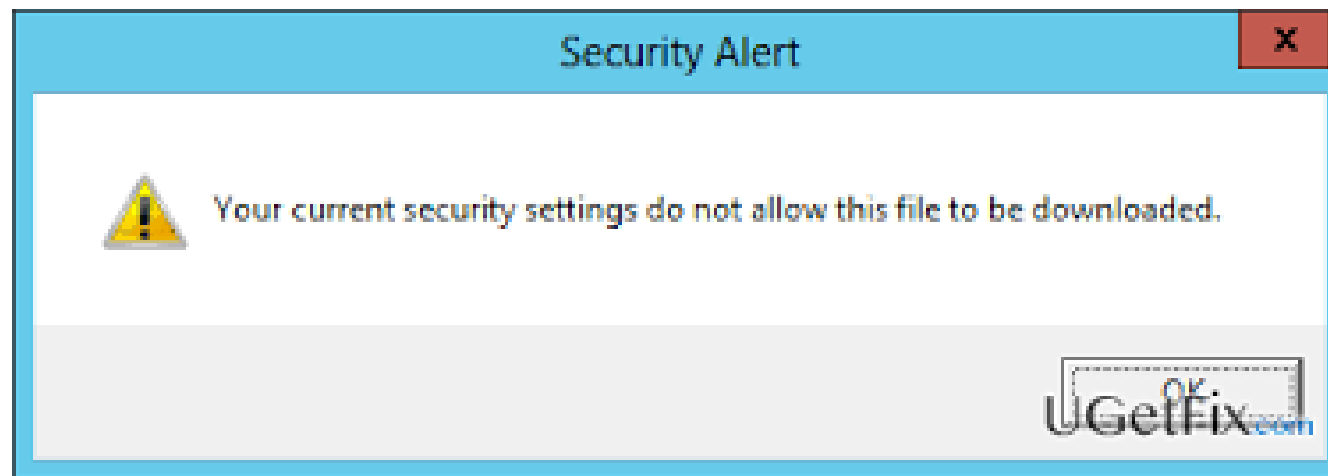
Control de entendimiento

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



Categoría: físico; Tipo: disuasorio, preventivo, correctivo

¿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.



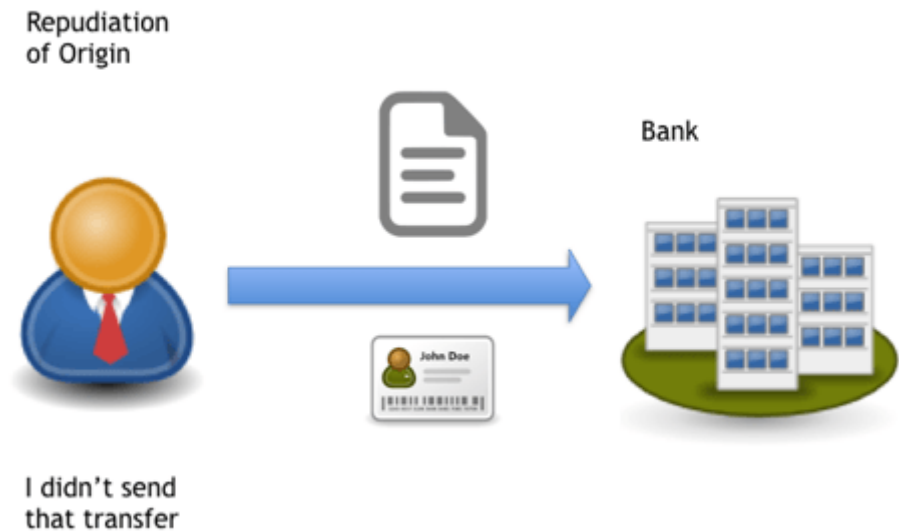
Va de la mano con la triada CIA

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.



¿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.