ZEROLYNX

Inverfin Holding - INSESO

Presentación Ejecutiva – Forense 202507 - 05/08/2025

Orden del día

- Objetivo del ejercicio realizado
- Hallazgos clave
- Análisis de cada acción realizada durante el ejercicio
- Opinión pericial
- Implicaciones y recomendaciones
- Validez del proceso forense
- Conclusiones finales

Contexto

EJERCICIO: OPINIÓN PERICIAL EXPERTA

INFORME EXPEDIENTE 2025/06

Ejercicio realizado en Mayo de 2025

Objetivo del ejercicio

- Análisis forense del servidor de INSESO.
- Verificación de logs y anomalías en sistema AGRESSO.
- Preservación de evidencias digitales críticas.

Fases

Objetivo Principal

- Clonación de servidor
- Análisis forense de logs
- Análisis de Agresso

Evaluación Adicional

- Análisis del estado actual de ciberseguridad
- Comparación frente a estándar

Ampliación por Incidencia

- Revocación de privilegios en el Directorio Activo
- Análisis de logs en la máquina afectada

Hallazgos clave

- Indicios de **acceso intencionado** con privilegios revocados.
- Usuario interno con conocimiento del sistema comprometido.
- **Registros del sistema eliminados** de forma deliberada.
- Usuario sospechoso identificado: Antonio Sánchez.
- Inconsistencias en los logs: **manipulación probable**.

Acciones realizadas durante el ejercicio

- Auditoría forense de logs.
- Análisis forense de particiones.
- Revisión de Agresso.
- Análisis GAP frente a estándar: CIS.

Auditoría forense de logs

10 marzo

09:40:20
Acceso existoso al sistema del usuario “RCENGONGA”

28 abril

13:57:49
Acceso de “Administrador@INSESO01.LOCAL”, seguido por “admbios”

20 mayo

Falla de ejecucuón de backup por CSV no disponible, detención de máquina virtual con fallo de replicación Hyper-V

21 mayo

15:50:18
Nuevo acceso de “RCENGONGA”

19:42:31 Intento fallido con cuenta “Administrador”, ya deshabilitada

Análisis de forense de particiones

Acceso del usuario identificado

Actividad sospechosa y clonación de datos atribuida a usuario identificado

04

01

Ficheros eliminados

Brecha temporal anómala sugiere possible borrado selectivo o resintalación del sistema

Evidencias temporales

Trazabilidad de usuario sospechoso hasta mayo de 2025

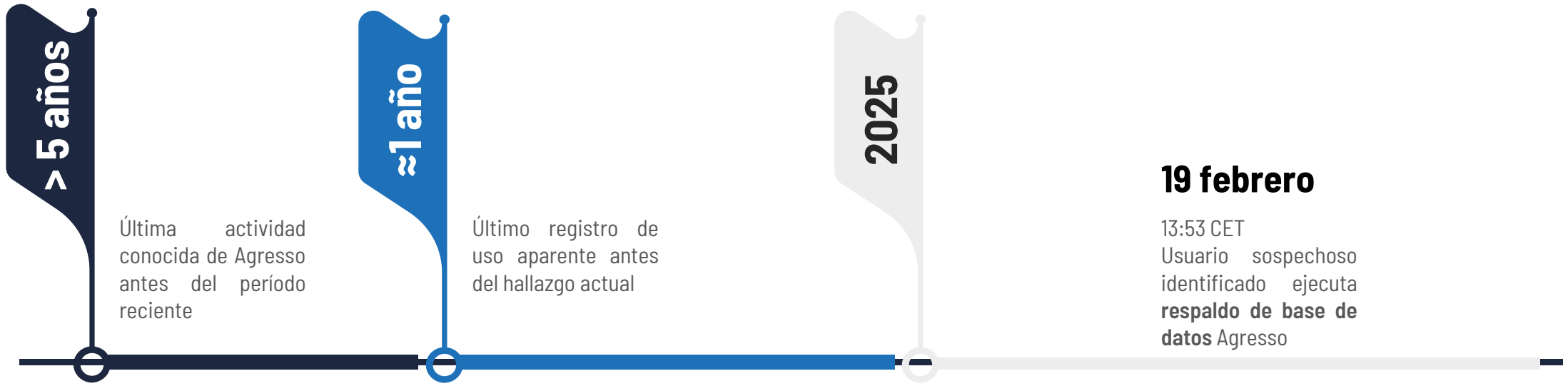
03

02

Exportación de bases de datos

Evidencia de exportacón de bases de datos a unitdad externa

Revisión de Agresso



- **Ficheros sensibles recuperados**:
  - Archivos eliminados contenían datos del sistema de pensiones.
  - Confirmada presencia de información institucional crítica.
  - Riesgo elevado en caso de fuga o manipulación.

19 febrero

Desde 08:00 CET
Actividad técnica sostenida durante la mañana

03 marzo

20:56 CET
Nueva actividad relacionada con Agresso detectada en el sistema

Análisis GAP frente a estándar: CIS

Protección de datos débil

Sin cifrado ni control de accesos; documentos sensibles en sistemas inseguros

Ausencia de validación técnica

No se realizan pruebas de penetración, escaneos, ni ejercicios de respuesta ante incidentes

Inventarios Incompletos

Sin control de dispositivos ni software, activos obsoletos o desconocidos en red

Falta de cultura de ciberseguridad

Sin formación ni conciencia sobre amenzadas digitales, alto riesgo de errores humanos

Parches deficientes

Software obsoleto, sin parches de seguridad aplicados y sin gestion de vulnerabilidades

Gestión inadecuada de accesos

Cuentas compartidas, privilegios excesivos y sin MFA; riesgos de accesos indebidos

Backups sin control

Copias de seguridad obsoletas o inexistentes; problemas de restauración

Fraude y Manipulación de evidencias

Intencionalidad de los actos

- Uso de Robocopy para copiar la base de datos de Agresso5.
- Indicador de intento de robo de información.

Destrucción de rastros digitales

- Vacío temporal de más de un año en archivos recuperables.
- 74,076 ficheros eliminados sin metadatos.
- Acciones deliberadas para ocultar ilícitos.

Sabotaje durante la auditoría

- Intento de conexión a la cuenta 'Administrador' deshabilitada.
- Atacante actuó de manera consciente y reactiva.

Conclusiones periciales

- El entorno digital de INSESO está comprometido.
- Urge actuar con rapidez y decisión política.
- Proteger datos ciudadanos es responsabilidad del Estado.

Implicaciones políticas

- Potencial daño legal y reputacional al Estado.
- Riesgo de sabotaje institucional y filtración de datos.
- Necesidad de supervisión política en ciberseguridad.

Recomendaciones

- Intervención urgente en sistemas críticos.
- Implementar controles de seguridad CIS.
- Capacitación interna en ciberseguridad.
- Supervisión política de la seguridad digital institucional.

Validez del Proceso Forense

- Profesionalidad del Informe de Zerolynx

Metodología empleada

Uso de estándares reconocidos (UNE, ISO)

- Preservación de la Cadena de Custodia

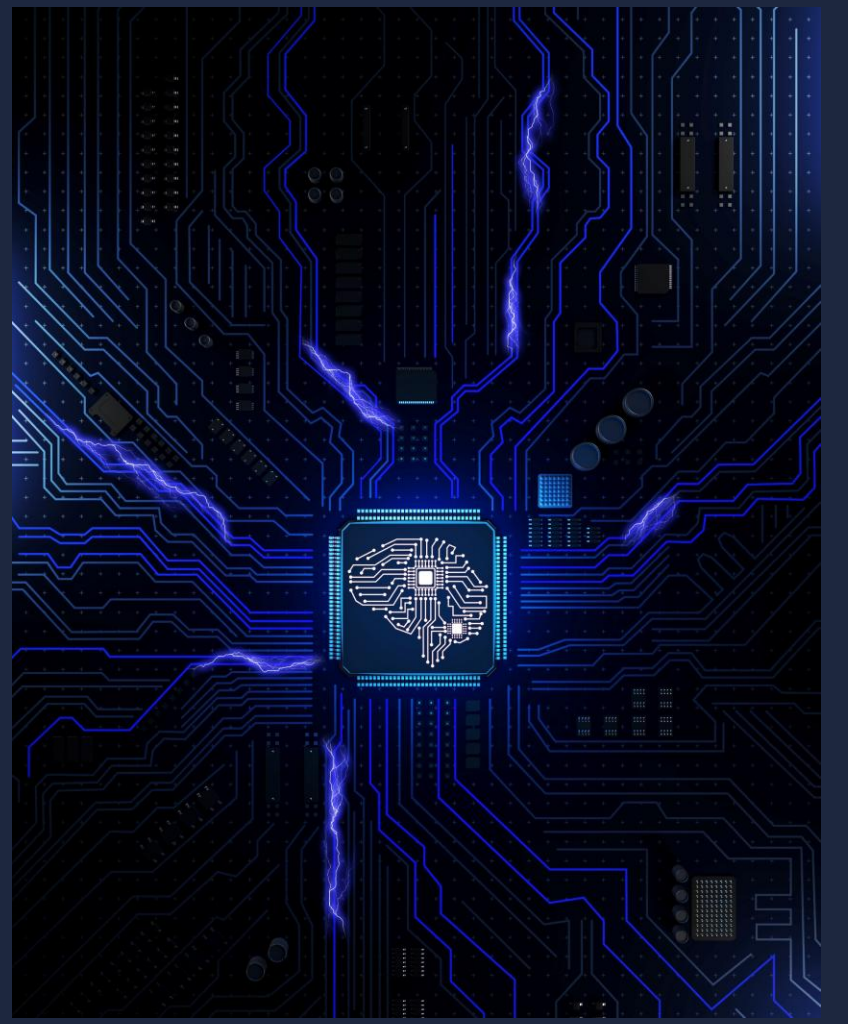
Correcta preservación de la cadena de custodia.

- Uso de Herramientas Forenses Estándar

Garantizada integridad, autenticidad y fiabilidad de las pruebas.

- Conclusiones Respaldadas por Evidencia Digital

Conclusiones sólidamente respaldadas



Conclusiones finales

Ataque Interno Deliberado
• Fines de fraude y sabotaje

Estado de Abandono Crónico
• Vulnerabilidad extrema en ciberseguridad

Intervención Urgente Necesaria
• Mitigar daños
• Establecer responsabilidades
• Implementar plan de remediación

Reconstrucción de Seguridad
• Infraestructura crítica para el país

Contáctanos


www.zerolynx.com


www.github.com/zerolynx


www.linkedin.com/company/zerolynx


@ZerolynxOficial

Zerolynx Oficial


blog.zerolynx.com