Informe Ejecutivo de Opinión Pericial

Orden del día

Introducción

Objeto del Informe

Síntesis de Hallazgos Clave

Opinión Pericial

Evaluación de Riesgo e Impacto

Recomendaciones Priorizadas

Conclusión Final

Fecha y Asunto

FECHA: 28 DE JULIO DE 2025

ASUNTO: OPINIÓN PERICIAL EXPERTA SOBRE EL INFORME FORENSE DEL EXPEDIENTE 202505/06 DE INSESO

Referencia

Referencia: "Informe forense pericial - Expediente 202505/06" emitido por Zerolynx S.L. con fecha 09/07/2025.

Destinatario y Remitente

Para: D. Roberto Nsue, CEO y Apoderado, Inverfin Holding S.A.

De: Empresa Experta Forense Independiente en TIC, Zerolynx

Objeto del Informe

Finalidad del Documento

- Ofrecer una opinión pericial experta
- Ser independiente y objetiva

Hallazgos del Informe Forense

- Documentados en el informe de referencia

Gravedad e Implicaciones

- Analizadas en el contexto del INSESO

Situación de Máxima Criticidad

- Situación de máxima criticidad
  - El informe revela una situación de alta gravedad
- Identificación de fallos de seguridad
  - Se han detectado múltiples vulnerabilidades
- Evidencias de actividad maliciosa
  - Pruebas concluyentes de acciones maliciosas
- Acceso privilegiado a los sistemas
  - El actor malicioso tenía acceso privilegiado

Fraude y Exfiltración de Datos

- Copia no autorizada de bases de datos sensibles
  - Base de datos afectada: Agresso
  - Gestión del sistema de pensiones del país

Sabotaje y Destrucción de Pruebas

Borrado Intencionado de Logs y Archivos

Pruebas irrefutables de eliminación de registros

Objetivo de ocultar actividades ilícitas

Ataque Deliberado Durante la Auditoría

Interrupción de servicios de INSESO

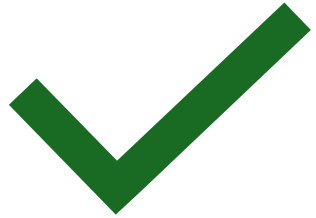
Ocurrió durante la propia auditoría

Colapso Sistémico de la Seguridad

Impacto Devastador del Ataque

El ataque fue posible debido a la falta de controles de seguridad

El impacto fue devastador



Estado de Abandono de los Controles de Seguridad

Incumplimiento de los controles de seguridad más básicos

Falta de cumplimiento de los Controles CIS4444

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

Fallas Sistémicas de Seguridad

Ceguera Operacional

Falta de un registro de auditoría centralizado y fiable

Imposibilidad de detectar el ataque a tiempo

Actividades ilícitas pasaron desapercibidas durante años

Fragilidad Extrema

Ausencia de un plan de copias de seguridad

Servicios tardaron días en restablecerse

Incapacidad de recuperación ante incidentes graves

Puertas Abiertas

Gestión laxa de accesos

Mantenimiento de cuentas de antiguos empleados

Provisión de credenciales necesarias al atacante

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
  - Garantizan integridad, autenticidad y fiabilidad de las pruebas
- Conclusiones Respaldadas por Evidencia Digital
  - Conclusiones sólidamente respaldadas

Confidencialidad de los Datos de la Ciudadanía

Riesgo Inminente y de Impacto Severo

Situación descrita representa un peligro significativo

Confidencialidad de los Datos de la Ciudadanía

Información personal comprometida

Datos financieros de los pensionistas afectados

Disponibilidad de Servicios Críticos

- Capacidad Operativa de INSESO
  - Probada como extremadamente frágil

Integridad y Reputación de la Institución

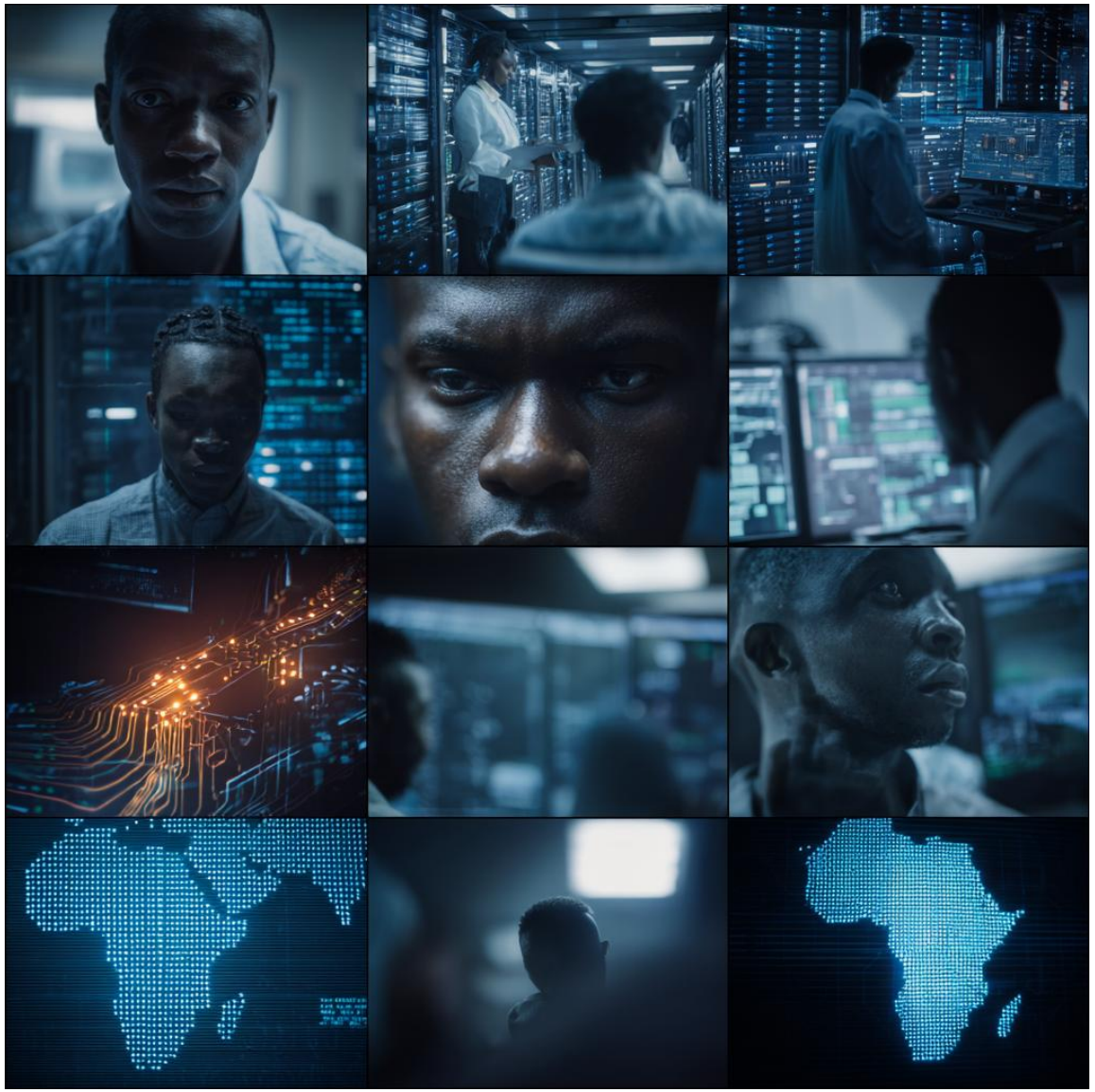
- Confianza pública dañada
  - Capacidad del INSESO para custodiar información en duda

Contención Inmediata

- Contención Inmediata
  - Aislar los sistemas comprometidos
  - Evitar más daños
  - Preservar las evidencias digitales
  - Preparación para un posible proceso judicial

Auditoría de Daños

- Investigación exhaustiva
  - Determinar el alcance total de la información exfiltrada
- Notificación a las partes afectadas
  - Informar a las partes si fuera necesario



Inventario y Control de Activos

- Importancia del Inventario y Control de Activos
  - Es fundamental para la protección de activos
  - Base de toda la estrategia de seguridad

Gestión de Accesos

Implementación de Autenticación Multifactor (MFA)

- Desplegar MFA para todos los accesos
- Especialmente importante para accesos remotos

Limpieza de Cuentas y Privilegios

- Realizar una limpieza exhaustiva de cuentas
- Revisar y ajustar los privilegios de acceso

Copias de Seguridad y Recuperación

Importancia de un Sistema de Backups

Garantiza la continuidad operativa

Proporciona seguridad ante fallos

Características de un Sistema de Backups Robusto

Automatización para evitar errores humanos

Pruebas periódicas para asegurar su eficacia

Implementación de Controles de Emergencia

IMPLEMENTACIÓN DE CONTROLES DE EMERGENCIA (CIS IG1)19:

Conclusión Final

Ataque Interno Deliberado	Estado de Abandono Crónico	Intervención Urgente Necesaria	Reconstrucción de Seguridad
• Fines de fraude y sabotaje	• Vulnerabilidad extrema en ciberseguridad	• Mitigar daños • Establecer responsabilidades • Implementar plan de remediación	• Infraestructura crítica para el país

Para Más Información **(Contacto):**

E-mail: Roberto.nsue@InverfinHolding.com / Téléphone: (+240) 222230874.- www.InverfinHolding.com

Dirección: Ctra. Malabo Aeropuerto, Edificio Ryesa, Planta 1, Malabo, Guinea Ecuatorial.

INVERFIN HOLDING ©,

Documento CONFIDENCIAL