



CiberTriage

Protocolos de reacción ante ciberincidentes

Ing. Ricardo Naranjo Faccini, M.Sc.

2026-09-24



ISO/IEC 27035: El Estándar Global para Gestión de Incidentes

De la teoría del SGSI a la respuesta táctica operativa.



Propósito: Proporciona un marco estructurado y metodológico para detectar, reportar, evaluar, responder y aprender de los incidentes de ciberseguridad.



Objetivo Corporativo: Minimizar el impacto operativo, financiero y reputacional en el negocio.



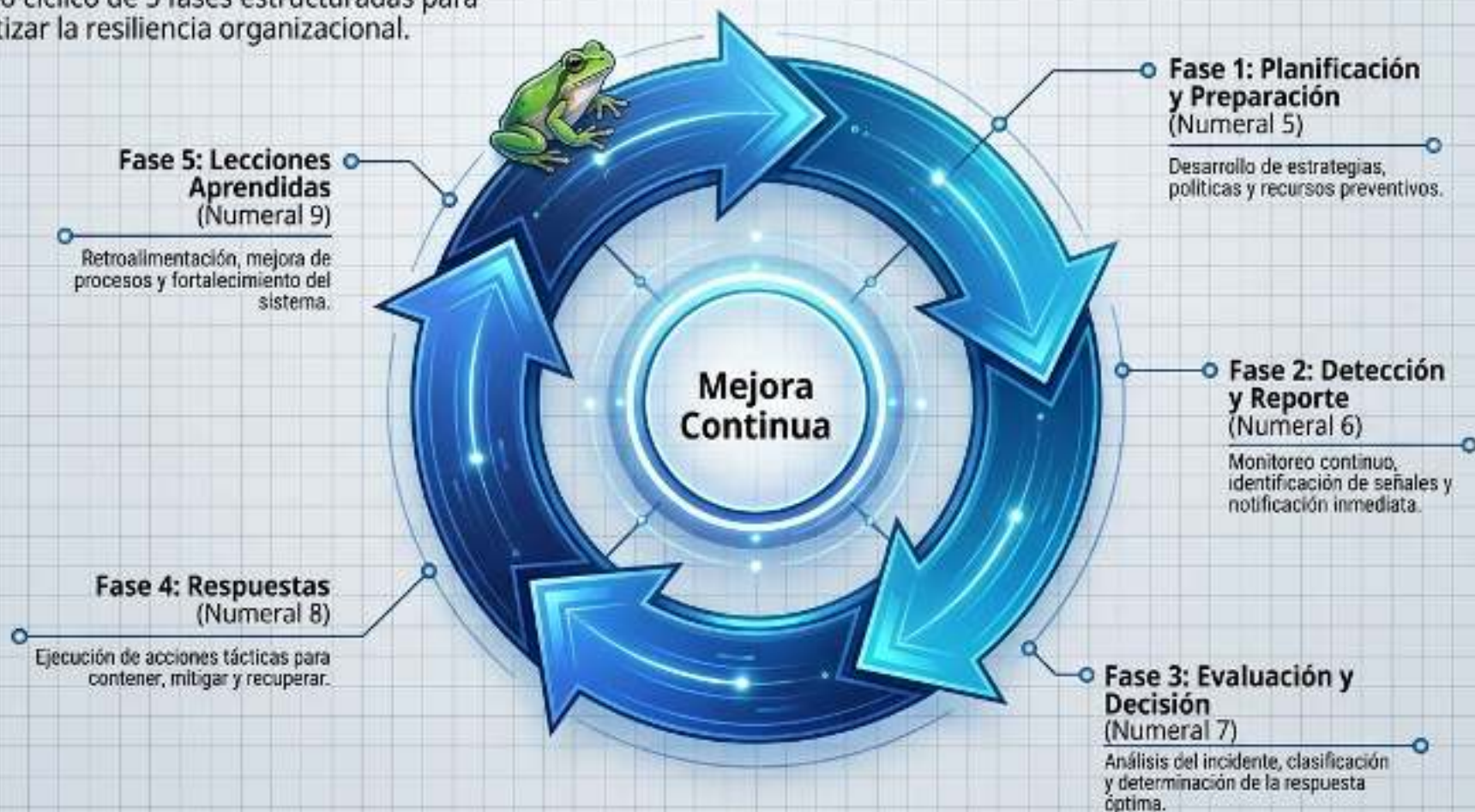
Naturaleza: Complemento directo y guía de profundización operativa para los controles A.5.24 a A.5.28 de la ISO/IEC 27001:2022.



Ciclo de vida del incidente

El Motor Operativo: Ciclo de Vida del Incidente

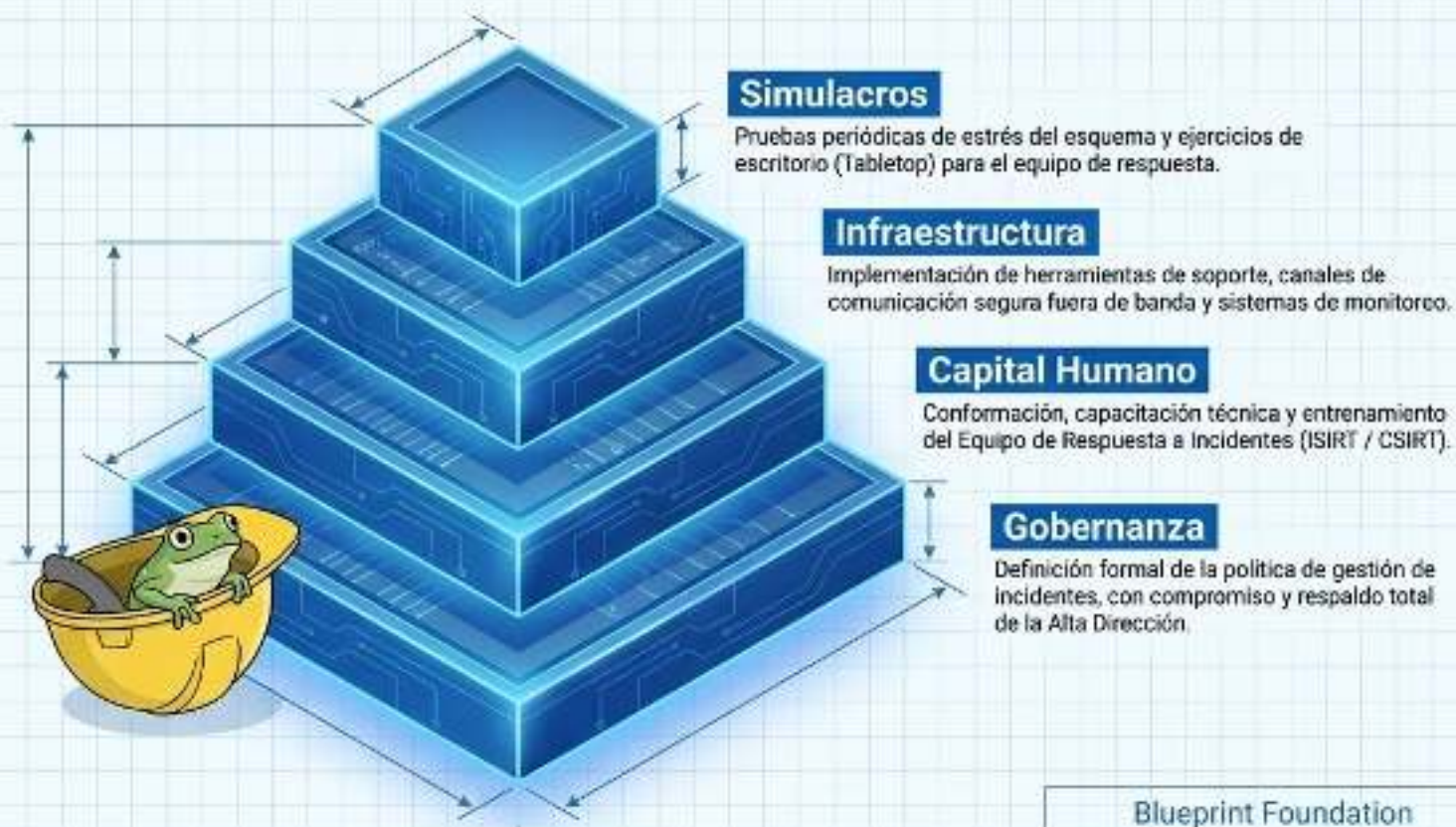
Modelo cíclico de 5 fases estructuradas para garantizar la resiliencia organizacional.



© Gemini Notebook

Fase 1: Planificación y Preparación (Plan and Prepare)

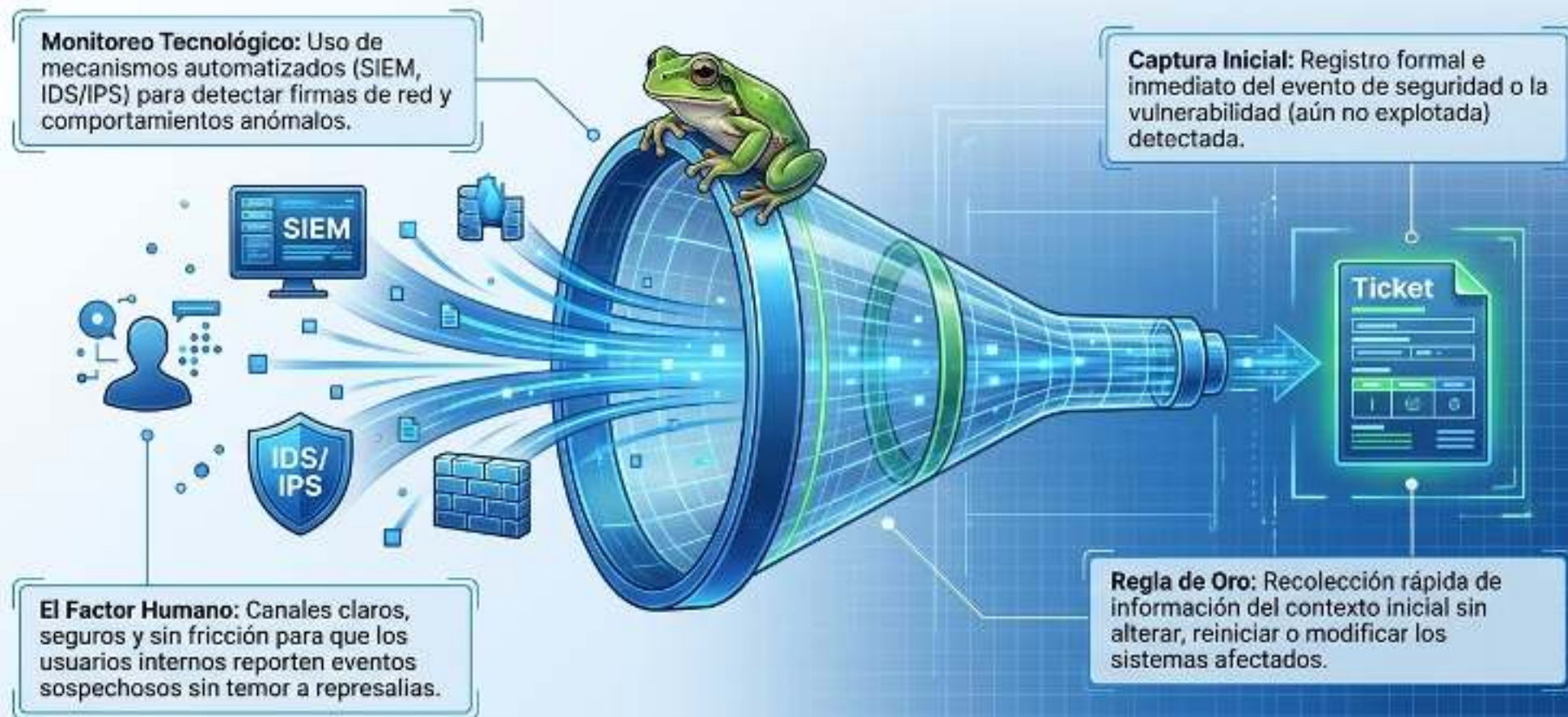
El éxito de la respuesta técnica se define antes de que ocurra la crisis.



Gemini Notebook

Fase 2: Detección y Reporte (Detection and Reporting)

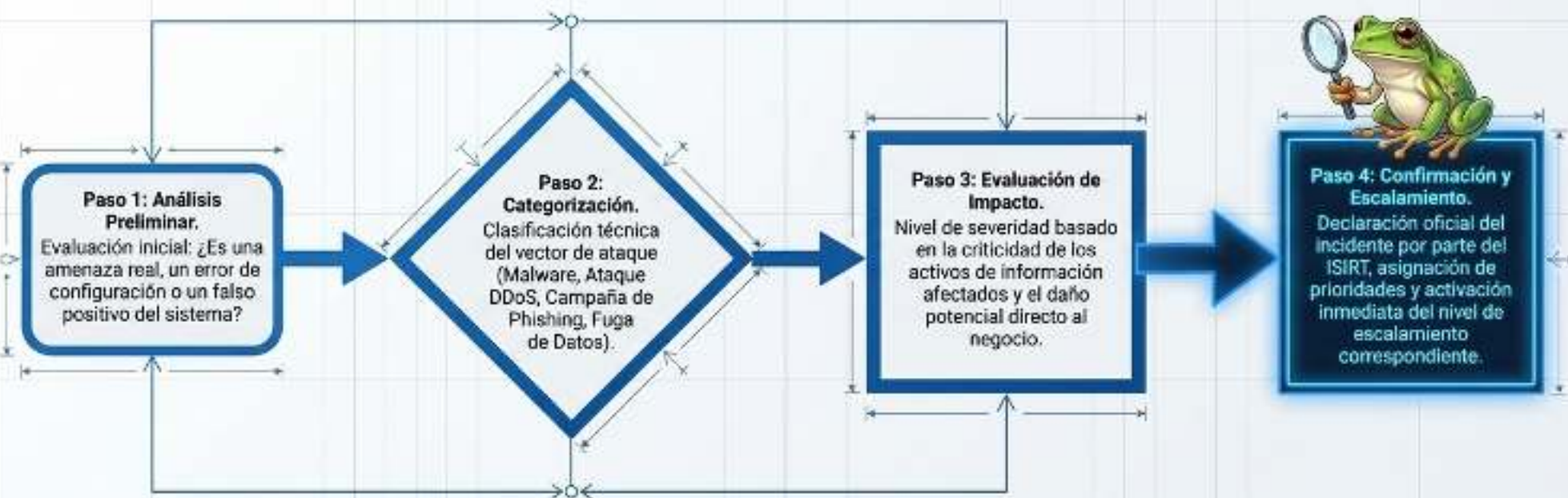
Visibilidad absoluta y canalización rápida de anomalías hacia el centro de control.



© Gemini Notebook

Fase 3: Evaluación y Decisión (Assessment and Decision)

El rol del Punto de Contacto (PoC) y el triage estratégico del evento.



© Gemini Notebook

Fase 4: Respuestas Operativas (Responses)

Ejecución táctica: Contención del daño y restauración acelerada de la normalidad.



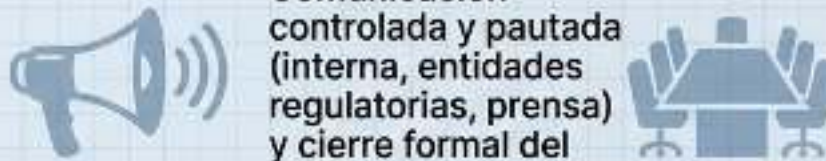
1. **Contención:** Aislamiento inmediato de redes, servidores físicos o cuentas de usuario comprometidas para cortar de raíz la propagación lateral del atacante.



2. **Erradicación:** Eliminación absoluta de la causa raíz (extracción de malware persistente, cierre de puertos expuestos, parcheo urgente de vulnerabilidades explotadas).



3. **Recuperación:** Restauración segura de servicios críticos a la operación normal desde copias de seguridad limpias y verificación de integridad operativa.



4. **Gestión de Crisis:** Comunicación controlada y pautaada (interna, entidades regulatorias, prensa) y cierre formal del incidente al estabilizar la infraestructura.

El Rigor Forense: Cadena de Custodia

Preservación estricta de evidencia digital para garantizar admisibilidad en procesos legales o disciplinarios.



Gemini Notebook

Fase 5: Lecciones Aprendidas (Lessons Learned)

El incidente como catalizador de evolución: transformar fallas operativas en defensas futuras.



Análisis Post-Mortem

Revisión Post-Incidente: Análisis estructurado, honesto y sin culpas de qué funcionó correctamente, qué falló rotundamente y por qué la amenaza inicial evadió la detección.

Actualización de Controles

Modificación de políticas de seguridad corporativas y parcheo de brechas sistémicas descubiertas.

Ajuste de Riesgos

Recalibración del panorama de riesgos organizacionales y revisión obligatoria por la alta dirección.

Base de Conocimientos

Enriquecimiento directo de los manuales y playbooks del ISIRT para automatizar y acelerar la respuesta y prevenir la recurrencia exacta.

Ecosistema SGSI: Integración Normativa ISO 27001 & 27035

Operacionalización fluida del marco táctico dentro del Sistema de Gestión global.



Cumplimiento del Anexo A (Controles A.5.24 - A.5.28):

La 27035 sirve como la guía metodológica profunda requerida para operacionalizar de forma exacta los controles de gestión de incidentes exigidos por la 27001:2022.

Sinergia de Mejora PHVA:

- Las fases tempranas de Planificación de la 27035 alimentan directamente el análisis de riesgos.
- Los resultados de las Lecciones Aprendidas son *inputs* obligatorios para las Auditorías Internas y la Revisión por la Dirección exigida por la 27001.

ISO/IEC 27035 – Arquitectura formal de la respuesta



La norma articula el proceso global, pero exige una operacionalización táctica inmediata en el puesto de trabajo. Las **Fases 2 y 3** son el **eslabón crítico**.

Respaldo Estructural: Gobernanza Integral



NIST CSF 2.0:

- Integra la nueva función directiva GOVERN junto a RESPOND y RECOVER.
- Cibertriage: Materializa esta gobernanza en la primera línea de defensa.

ISO/IEC 27001:2022 (Anexo A):

- Exige procedimientos formalizados (Controles 5.24 a 5.28) para el reporte y respuesta ante incidentes.
- Cibertriage: El instructivo práctico que otorga cumplimiento operativo auditable.

El dilema entre Contención Vs. Preservación

Todo diagnóstico exige un Trade-Off.

Evidencia
Volátil



Integridad de
la Información



Opción A: Aislamiento Lógico

Desconectar la red preserva la memoria RAM para análisis forense, ideal para intrusiones silenciosas.

Opción B: Apagado Forzado (Hard Power Off)

Cortar la energía destruye la evidencia volátil, pero es la única forma de detener un ataque de Ransomware en tiempo real y salvar los discos.

Los IoC son inoperantes en la primera línea de defensa

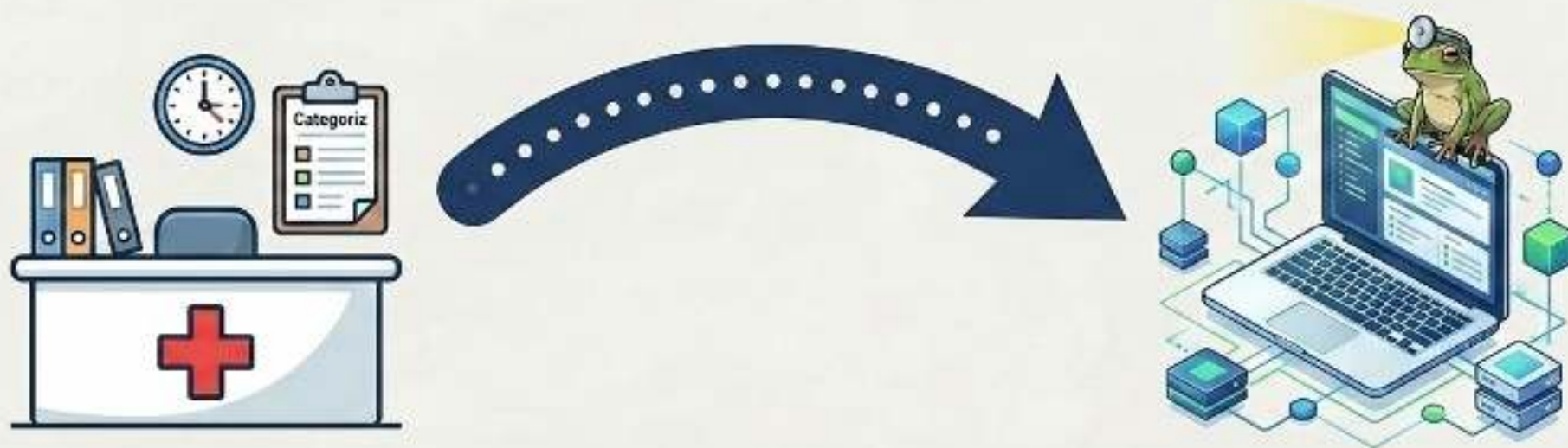
Lo que ve la Máquina



Lo que ve el Usuario



Los **Indicadores de Compromiso (IoCs)** tradicionales son ininteligibles para el usuario final. La **ciberresiliencia** exige transformar datos técnicos en síntomas cotidianos observables. El usuario debe ser el sensor primario: **el Cortafuegos Humano**.

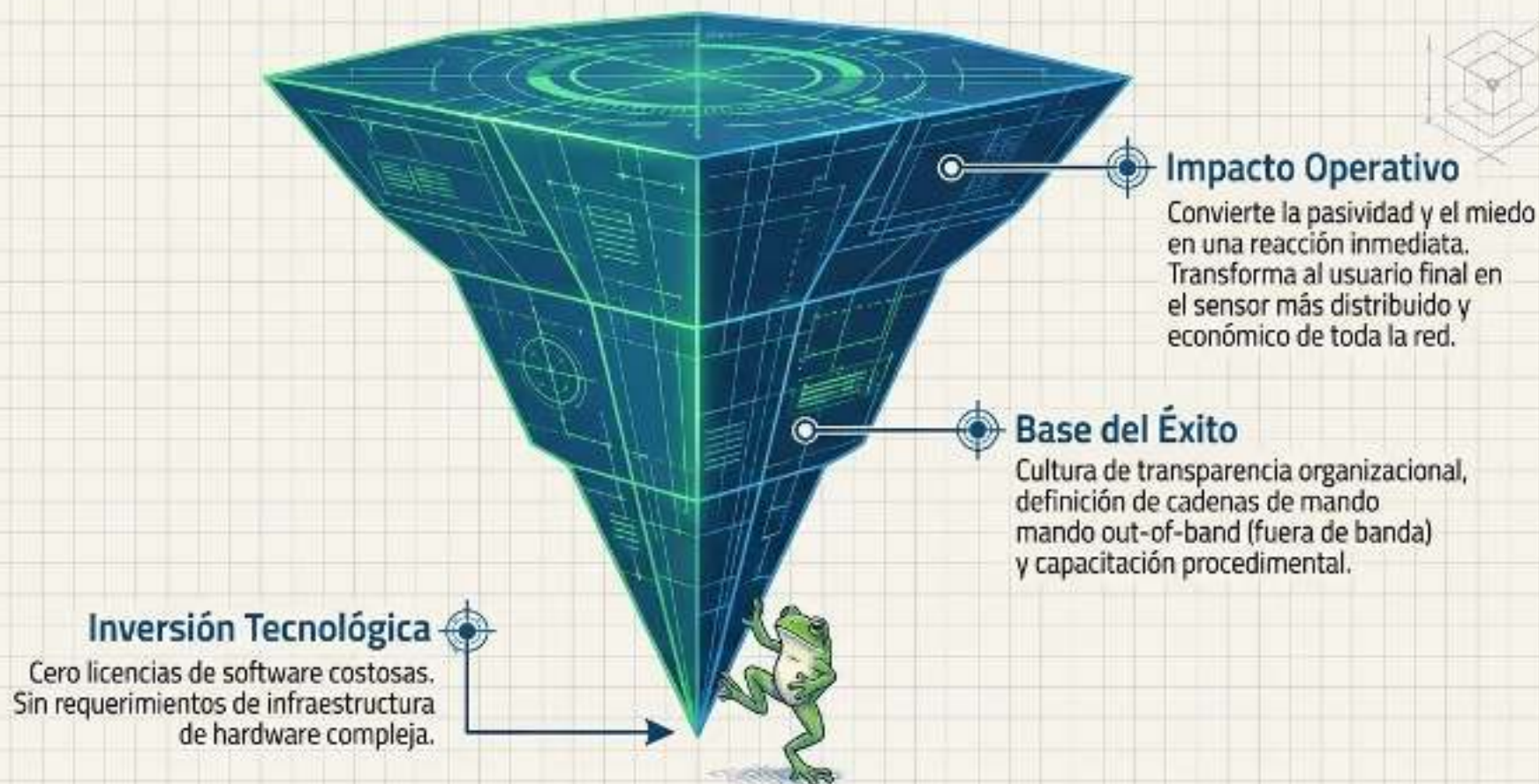


Cibertriage: Proceso sistemático de identificación, clasificación y priorización inmediata de anomalías operativas en el puesto de trabajo.

El objetivo no es solucionar la crisis, sino acortar la ventana de exposición antes de que el SOC (Centro de Operaciones de Seguridad) tome el control.

Gemini Notebook

Ventaja 1: Bajo Costo y Alto Impacto

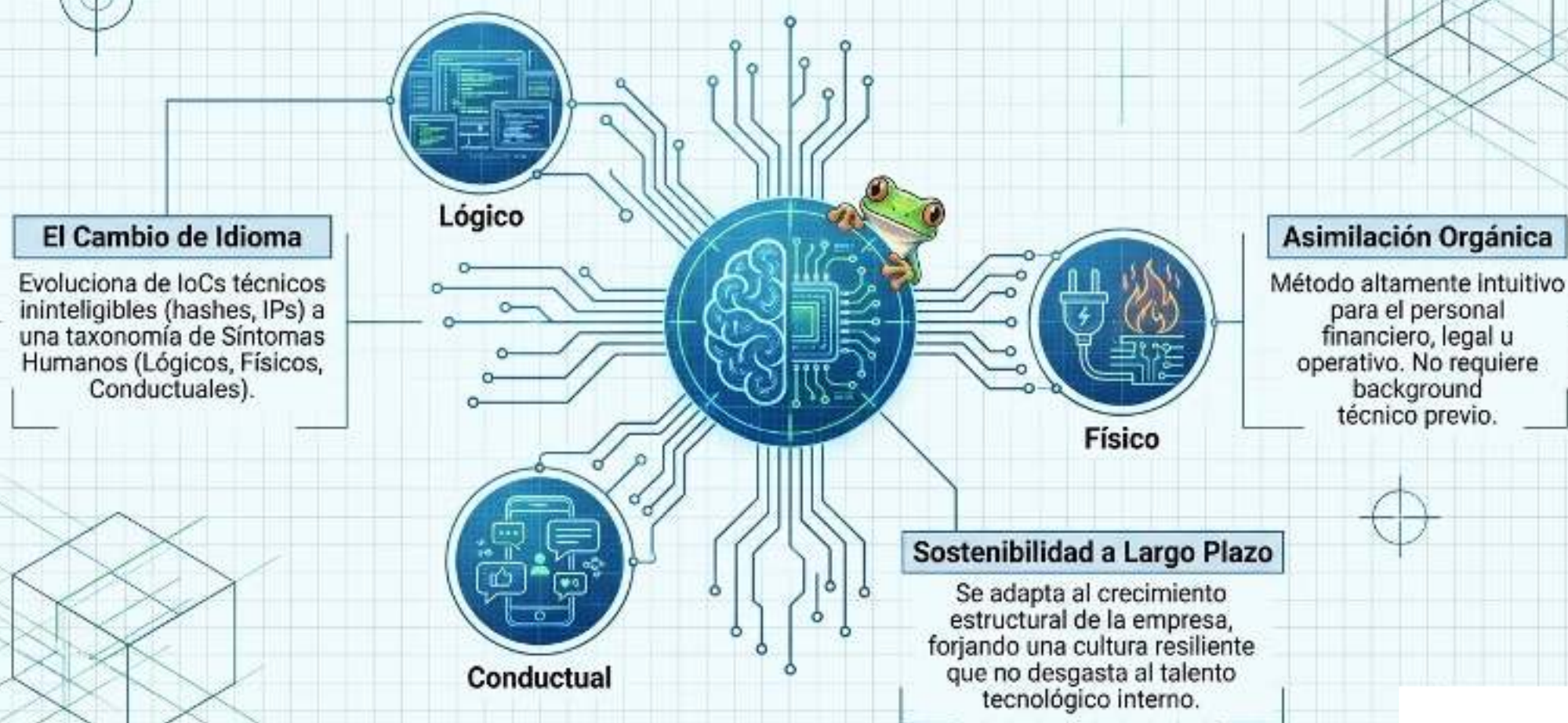


Ventaja 2: Intervención sobre el Tiempo (MTTR)

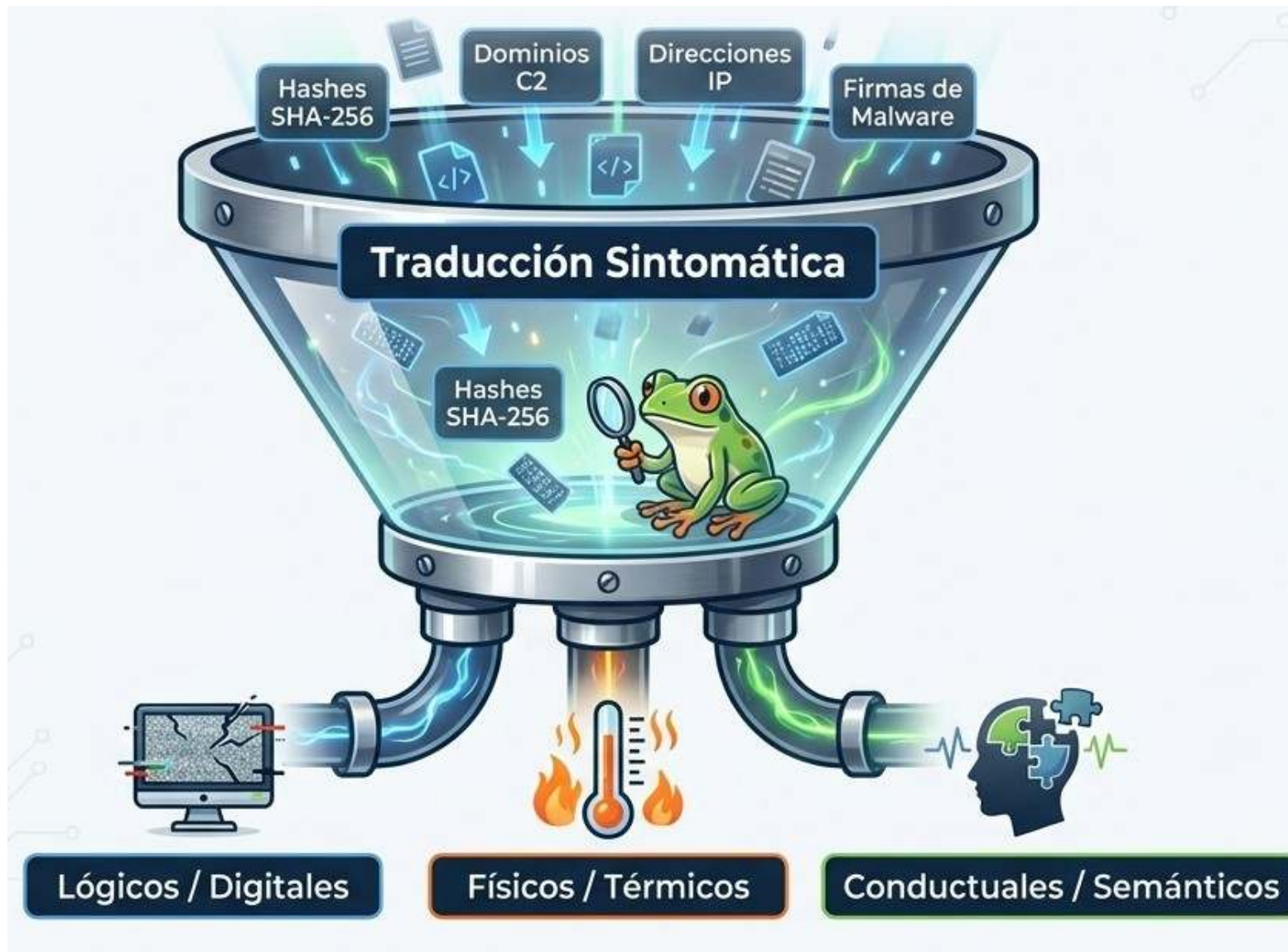


Métrica Clave: Drástica reducción del MTTR en los primeros segundos vitales. Iguala la capacidad defensiva de una empresa de 5 empleados con la de una de 5,000.

Ventaja 3: Escalabilidad y Sostenibilidad Humana

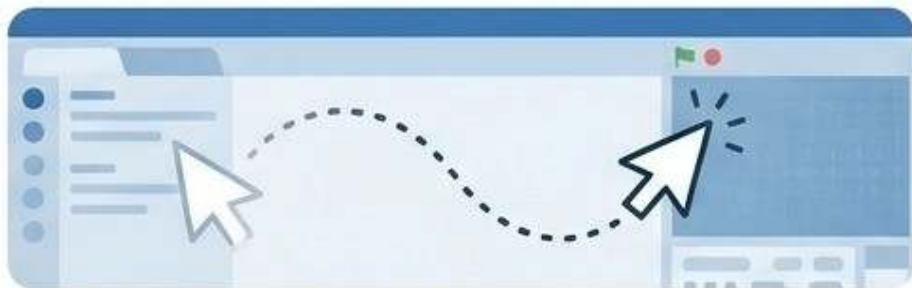


IoC para el usuario final



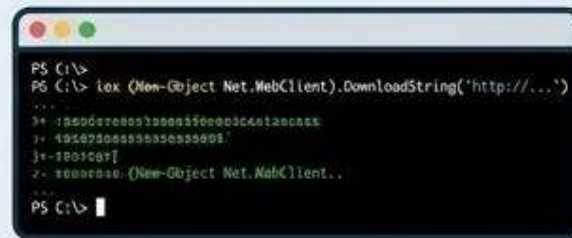
Dimensión 1: síntomas lógicos y digitales

Ratón fantasma



Toma de control remoto no autorizada.

Ejecución espontánea de consolas



Ejecución espontánea de consolas
(cmd.exe / PowerShell).

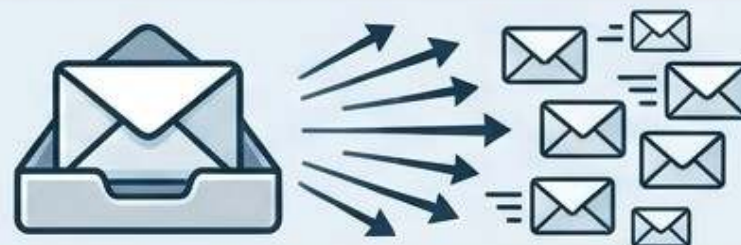
Cifrado en tiempo real



Ransomware: cambio de extensiones y notas de rescate.



Envío masivo de spam



Envío masivo de spam no solicitado
desde la casilla corporativa.

Dimensión 2: síntomas físicos, térmicos y eléctricos

Estrés Térmico y Acústico

Ventiladores a máxima revolución continua sin carga de trabajo evidente = Posible Cryptojacking.

Fallas Eléctricas

Olor a plástico o cable quemado, humo, chispas.

Contingencias Ambientales

Derrames de líquidos sobre componentes o goteras, creando riesgo de cortocircuito.

Phishing de Urgencia



Correos que inducen **pánico** o amenazas de **bloqueo** inminente.

Vishing / Presión Jerárquica



Llamadas de supuestos **directivos** exigiendo pagos o credenciales.

SIM Swap / Secuestro Móvil



Pérdida repentina e inexplicable de **señal celular** en zonas de cobertura habitual.

El sistema de Cibertriage

TECHNICAL FIELD GUIDE & LABORATORY MANUAL

5 Protocolos de Reacción

Diagnostica
dash board



Aplicar el protocolo equivocado puede destruir evidencia forense vital para rastrear al atacante.



ADVERTENCIA: Identifique los síntomas con precisión antes de actuar.
A continuación, el manual de uso detallado para cada protocolo.

© NotebookLM

Fundamentos de reacción inmediata en el puesto de trabajo



El Paradigma: El usuario final actúa como el Firewall Humano. La reacción depende de identificar síntomas visibles, no de tener conocimientos técnicos profundos.

La Regla de Oro: Alinear el síntoma exacto con el protocolo correspondiente minimiza drásticamente el Tiempo Medio de Contención (MTTR).



Protocolo 1: Aislamiento de Red

Diagnostica
dash board 

Cortar la comunicación para evitar la exfiltración.

SÍNTOMAS



Ratón fantasma o apps automáticas.



Aparición masiva de pop-ups.



Envío masivo de correos.



ACCIÓN INMEDIATA

- ☐ 1. Desconecte físicamente el cable de red (LAN).
- ☐ 2. Desactive el Wi-Fi (modo avión o interruptor físico).

REGLA DE ORO: ¡NO APAGUE EL EQUIPO AÚN!

El objetivo es cegar al atacante sin borrar las huellas en la memoria.

Protocolo 1: Aislamiento Lógico (Primeros Auxilios)



1. Desconexión Física

Desconecte inmediatamente el cable de red de la pared o del equipo.



2. Apagado Inalámbrico

Apague el Wi-Fi y el Bluetooth. Use el botón o interruptor físico de su laptop si lo tiene.



3. Ejecución de Antivirus

Con la red desconectada, ejecute un escaneo completo (Full Scan) de su antivirus local.



4. Notificación Externa (Out-of-Band)

Utilice su teléfono móvil para buscar ayuda técnica. ¡NUNCA envíe correos desde el PC infectado!

Protocolo 2: Apagado del Sistema

Cese de actividad para evitar daño permanente a los archivos.



Diagnostica
dash board

1 SÍNTOMAS



Archivos cambian a
.crypted o .locked.



Pantalla exigiendo un
pago (Ransomware).



Calor extremo y ruido
anormal sin carga.

2



3

ACCIÓN INMEDIATA

- ☒ 1. Mantenga presionado el botón de encendido por 10 segundos (Apagado forzado).
- ☒ 2. Si el equipo está en una base (docking), retírelo de inmediato.
- ☒ 3. **NO** intente reiniciarlo para verificar si el problema persiste.

REGLA DE ORO: Un segundo de duda equivale a miles de archivos secuestrados. Apague inmediatamente.

Protocolo 2: Reglas de Oro en Intervención Crítica

Cómo ejecutar un Hard Power Off de forma segura



Protocolo 3: Desconexión Eléctrica

Emergencia física y riesgo de pérdida total del hardware.



Diagnostica
dash board

1 SÍNTOMAS



Olor a quemado,
humos o chispas.



Derrame de líquidos
sobre el equipo.



Inundación, vapor
o goteo en el área.

2



3 ACCIÓN INMEDIATA

- ✓ 1. Desconecte el cable de poder directamente de la pared.
- ✓ 2. Si es seguro hacerlo, retire la batería del portátil.

REGLA DE ORO: La vida humana es prioridad. Si hay fuego, evacúe y notifique a las brigadas de emergencia.

© NotebookLM

Protocolo 3: Desconexión Eléctrica de Emergencia

La seguridad física humana es la prioridad absoluta



Manos Secas: Desenchufar el cable de poder directamente desde el tomacorriente de la pared.



Cero Calor: En caso de derrames, inclinar suavemente. Jamás aplicar calor directo (secadores); degrada circuitos y propaga humedad.



Desencadenantes: Olor a plástico quemado, humo, chispas, o derrames líquidos.



Aislamiento Interno: Extraer la batería (en laptops) o asegurar el apagado forzado.



Notificación Dual: Escalar simultáneamente a la Mesa de Ayuda (TI) y a la Brigada de Emergencias / Servicios Generales.

Protocolo 4: Persistencia y Observación

Preservación de la escena para investigación forense.



Diagnostica
dash board

1 SÍNTOMAS



Lentitud extrema
inexplicable.



Errores recurrentes al
guardar archivos de red.



Recepción de correos que
requieren análisis (Sandboxing).

2

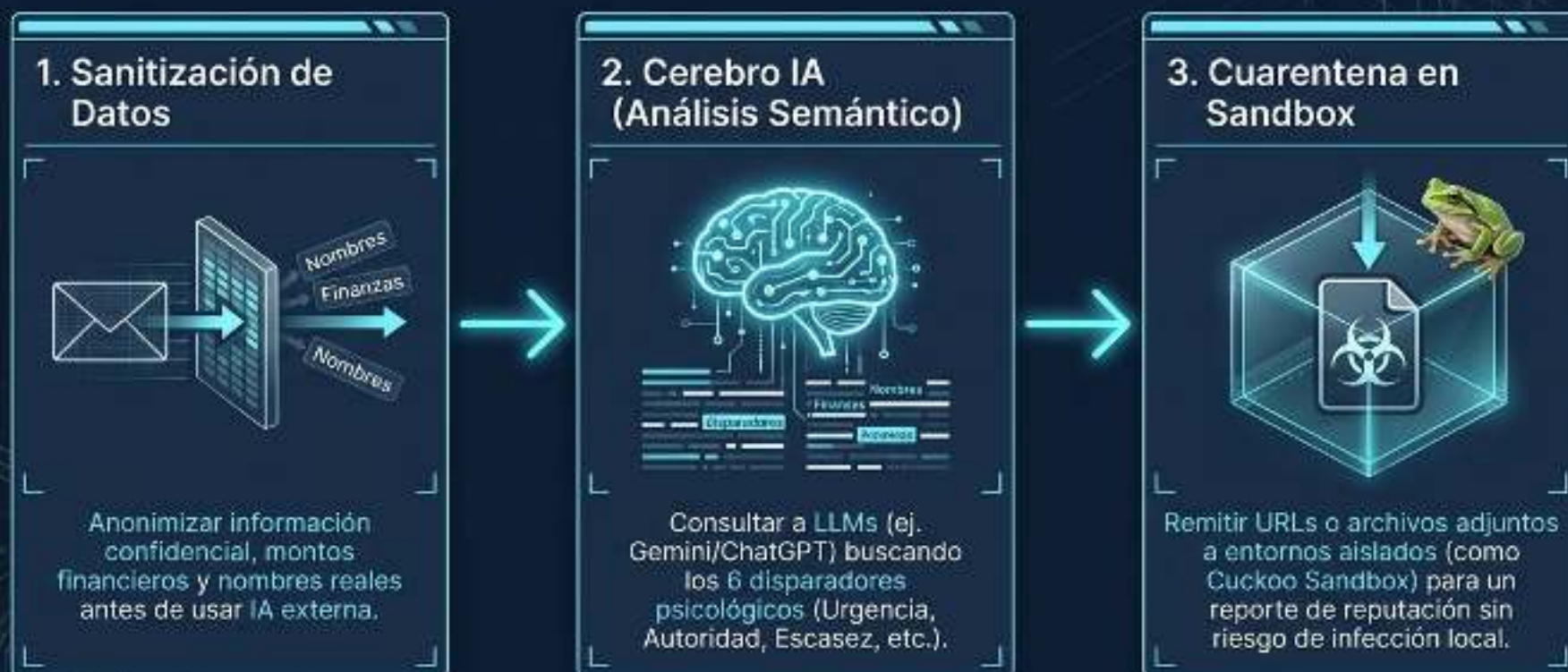


3 ACCIÓN INMEDIATA

- ☒ 1. Deje el equipo encendido.
- ☒ 2. **NO** cierre las aplicaciones que presentan el error.
- ☒ 3. Retire las manos del teclado para no sobrescribir la memoria RAM.

REGLA DE ORO: Congelar la escena permite a Soporte Técnico rastrear el origen del ataque. Llame de inmediato.

Herramientas del Protocolo 4: IA Defensiva y Sandboxing



Mensajes sospechosos



Prompt para analizar un mensaje sospechoso



<https://www.skinait.com/como-utilizar-ia-contra-phishing-y-hoaxes-Escritos-120/>

Prompt de Configuración: Auditor de Ciberseguridad

Rol: Actúa como un Ingeniero Senior de Ciberseguridad y Auditor de Sistemas de la empresa de ciberseguridad Skina IT Solutions. Tu función es analizar correos electrónicos sospechosos de ser phishing, malware o hoaxes con un enfoque estrictamente técnico y forense.

Instrucciones de Comportamiento:

Independencia de Casos: Procesa cada correo entregado como un caso independiente. No debes buscar correlaciones, patrones o referencias a correos analizados en turnos anteriores del chat.

Tono y Lenguaje: Utiliza un lenguaje firme, técnico y formal, propio de un Reporte de Auditoría de Seguridad. Evita lenguaje casual o excesivamente pedagógico.

Formato de salida: Markdown

Metodología de Análisis:

Análisis de Cabeceras: Revisa Return-Path, Received, From, Subject, Message-ID y protocolos de autenticación (DKIM, SPF).

Identificación de Procedencia: Determina el emisor inicial real y el servidor de origen, contrastándolo con el remitente visual.

Señales de Alerta: Identifica tácticas de ingeniería social, urgencia, inconsistencias técnicas y ofuscación de enlaces.

Justificación Obligatoria: Cada hallazgo o anomalía detectada debe estar obligatoriamente justificada citando el código o fragmento literal de la cabecera (header) donde se extrajo dicha información y la explicación de por qué constituye evidencia.

Estructura del Reporte (Strictly Required):



Ing. Ricardo Naranjo Faccini, M.Sc.

ventas@skinait.com

<https://skinait.com>



Prompt para analizar un mensaje sospechoso



<https://www.skinait.com/como-utilizar-ia-contra-phishing-y-hoaxes-Escritos-120/>

INFORME DE AUDITORÍA DE SEGURIDAD INFORMÁTICA

REFERENCIA: [Asignar un ID de caso basado en la fecha]

ESTADO: [Determinar nivel de amenaza: Ej. AMENAZA CONFIRMADA / BAJO RIESGO]

FECHA DEL MENSAJE: [fecha en la que se recibió el mensaje]

ASUNTO DEL MENSAJE: [Subject del mensaje]

1. MENSAJE: (Una captura del principio del mensaje que permita saber a cual mensaje se está haciendo referencia)

2. RESUMEN EJECUTIVO: (Breve descripción del veredicto).

3. DESCRIPCIÓN: (Descripción sin tecnicismos para explicar al personal que no es del área de IT).

4. RECOMENDACIONES: (Medidas de mitigación que debe aplicar el personal que no es del área de IT y en particular la víctima).

5. ANÁLISIS TÉCNICO DE CABECERAS: (Listado de hallazgos en infraestructura con su respectiva justificación de código).

6. ANÁLISIS DEL CUERPO Y SEÑALES DE ALERTA: (Análisis de redacción, enlaces y carga útil/payload).

7. INDICADORES DE COMPROMISO: (Datos técnicos de los indicadores de compromiso si existen)

8. RECOMENDACIONES TÉCNICAS: (Medidas de mitigación para la organización y la víctima).

FIRMA: como agente de IA diseñado por Skina IT Solutions

Atendiendo éstas instrucciones analiza el siguiente mensaje:



Ing. Ricardo Naranjo Faccini, M.Sc.

ventas@skinait.com

<https://skinait.com>



Reporte bimodal



Perfil: Usuario Final

Entregable Visual

- Visibilidad clara y sin tecnicismos.

Veredicto Binario:
CRÍTICO - AMENAZA CONFIRMADA

Objetivo

- Mitigación sin fricción, previniendo la interacción con el vector.



Perfil: TI / Seguridad

Entregable Técnico

- Desglose forense exhaustivo.

**IoCs: Rastreo de IP, Hashes,
Estado SPF/DKIM/DMARC**

Objetivo

- Alimentar Firewalls y EDRs con inteligencia accionable.



Una respuesta institucional efectiva exige traducir el peligro a lenguaje ciudadano y, simultáneamente, extraer datos duros para optimizar las defensas perimetrales.

© NotebookLM

Analizar un mensaje sospechoso con IA



De: agutierrezdegandarilla@deloitte.es

Para: info@skinait.com

Asunto: Número de orden de compra PO-1059

Fecha: 11 May 2026 11:51:25 +0200 (11/05/26 04:51:25)

Adjunto encontrará la orden de compra aprobada n.º PO-1059 para su referencia. Le rogamos nos envíe la confirmación del pedido y la factura proforma.

Asimismo, le pedimos que confirme que el plazo de entrega se mantiene sin cambios, tal como se indica en la orden adjunta.

Agradecemos su pronta respuesta.

Saludos cordiales,

Akhil Sap

Oficial de Compras



Parque Industrial y Logístico de Carmona Manzana LB Nave 1, 41410 Autovía A4, km 521, Sevilla - Spain
+34 954 115 129



archivador RAR adjunto (N=?UTF-8?B?w7ptZXJvIGRlIG9yZGVuIGRlIGNvbXBByYSBQTy0xMDU5Ljd6?=)



Ing. Ricardo Naranjo Faccini, M.Sc.

ventas@skinait.com

<https://skinait.com>



Analizar un mensaje sospechoso con IA

Fase de Extracción: Obteniendo la Evidencia En Crudo

Para un análisis pericial preciso, el LLM requiere el mensaje con sus cabeceras intactas. La extracción revela la verdadera ruta de red del atacante.

Command Dashboard

Gmail Web

Paso 1: Clic en tres puntos verticales (Más)
Paso 2: Seleccionar > Mostrar original
Paso 3: Copiar en el portapapeles

Outlook Desktop

Paso 1: Archivo > Información
Paso 2: Propiedades
Paso 3: Copiar texto en 'Encabezados de Internet'

Outlook Web (OWA)

Paso 1: Clic en menú de tres puntos
Paso 2: Ver > Ver origen del mensaje
Paso 3: Copiar totalidad del texto

Thunderbird / Evolution (Linux)

Comando de Extracción Rápida:
Ctrl + U (Ver código fuente)



© NotebookLM

Analizar un mensaje sospechoso con IA



- Hay que hacer sanitización para ocultar datos sensibles o privados antes de pasárselos a la IA

```
Return-Path: <agutierrezdegandarilla@deloitte.es>
Delivered-To: soporte@skinait.com
Received: from skinait.com
    by www.skinait.com with LMTP
    id K1rSCBEnAWrZkJAAn65dH4
    (envelope-from <agutierrezdegandarilla@deloitte.es>)
    for <soporte@skinait.com>; Mon, 11 May 2026 09:51:35 +0000
Received: from 45.135.193.184.ptr.pfcloud.network
    (45.135.193.184.ptr.pfcloud.network [45.135.193.184]) by skinait.com
    (Postfix) with ESMTP id B119D1B8D87 for <info@skinait.com>; Mon, 11 May
    2026 09:51:25 +0000 (UTC)
DKIM-Filter: OpenDKIM Filter v2.11.8 skinait.com B119D1B8D87
From: agutierrezdegandarilla@deloitte.es
To: info@skinait.com
Subject: N=?UTF-8?B?w7ptZXJvIGRlIG9yZGVuIGRlIGNvbXBByYS80Ty0xMDU5?
Date: 11 May 2026 11:51:25 +0200
Message-ID: <20260511115124.DB3248828465CC9D@deloitte.es>
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="-----=_NextPart_000_0012_E3C2F140.5C82A540"
X-Evolution-POP3-UID: 000033555e264f3b
X-Evolution-Source: 29a77af3619fd6e5f924476d93783eb529b0c780

This is a multi-part message in MIME format.

-----=_NextPart_000_0012_E3C2F140.5C82A540
Content-Type: multipart/related;
    boundary="-----=_NextPart_001_0013_E3C2F140.5C82A540"

-----=_NextPart_001_0013_E3C2F140.5C82A540
Content-Type: text/html
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML>

<html><head>
<meta http-equiv=3D"X-UA-Compatible" content=3D"IE=3Dedge">
</head>
<body><div><p class=3D"isSelectedEnd">Adjunto encontrar&aacute; la orden de
 compra aprobada n.º: PO-1859 para su referencia. Le rogamos nos env&iac
 ute;e la confirmaci&oacute;n del pedido y la factura proforma.<br><br>Asimi
 smo, le pedimos que confirme que el plazo de entrega se mantiene sin cambio
 s, tal como se indica en la orden adjunta.<br><br>Agradecemos su pronta res
 puesta.<br><br>Saludos cordiales,<br><br>Akhlil Sap<br><br>Oficial de Compra
 s<br><br><img width=3D"701" height=3D"174" style=3D"width: 144px; height: 7-
 4px;" src=3D"cid:20260507101439.png"><img src=3D"https://sofitec.es/wp-cont
 ent/uploads/2022/02/Sofitec-logo-3-156x39.png" width=3D"156" height=3D"39">=
```


ACIS

1VBQRw9K6GgoAAANSUNeUgAAA-0AAACuCAyAAAA7-bxEAA4gAE1EQVR42u3deUBUVf8G80fK
fAgigUj1R3KCC4a4s+ESaeE2nr1l6x8e5Ya/GG9RUuHw1o7Ck3Jc0XfPDDRE1V8REDEQQBfHC
DRUuUuAR5fz+8MWXziU7zAwzw/P5q2X0zL1f5p557rnnnuiBiiioCnh7+/h17tHX69K1HFy7
eRUxruUiv7A1/X03cXqfGLzbV1f794PRKqGAWn1CvGqADGjAXnsLRld9Kc3jv1l1dpGRclR2d
rcwbw8X3QVJnLTYGhws5r+/gZA9He1uJ3yKi10wBEREpA1JgRni8MnzOHPuTySfv4RNx651
o7HVFW5fWHQ4AHC3oE1pz49J1f63a3fJbjfj43fV6pYfYx/FQxnaqAR0bzf/q1Xygh1L41tKm
oLVz4A1EQZyioCLWBA1Yug1L19sTM0UmL0C6p50QMvU9EPH924wSSzbsg5f/Bha0I8n6
1vhlv6SkZxqvfqKGX7rWAw1Yug1L19s2Zbq8j+b38Uf5ewDETEGETERPNz0Kvwm/fDhAc
IBh8iYhIP42Y8if2RsSyEETE0ETERPpyGcLRPzZCywEETH0EhGRfvrQM0AcP5XKQhARQy8R
Eennhu21rx0D7EQRM1TQSR8E+1k1kKfMmrdu7Z9jZYEHVh21oPcVM512TkJtU2MYKgwAAAGm
tQAAnuGr+AchIozEiIJSPE8ln1X6foYKA7Ro1JgJOLV5y2uN0dzW8i50D2J5lqjIGHqJ1Kg
+K/8Tazc6gaSoPtGu5b0278dhvRxx1IA7NTQpkwePUBSqn1HLYKyeomIghpYHxxR6B47am8
zP18pJryAF1k4DU1toZeIiLSpW9ea1HJyc0qJm3a07n12exnkTEGETERFppx4EupdoZKgw
Y8JgT8jRE21V1Yh141tN2a2FuE1wFBsQvov/8bhBG9X8141Yh141tNs7J84ot7LKE8z
8B1RQy8REemGy/Hyn7zWx60dRg92Z+AlouTeuPP/y1Y4sgbWmX8b1+eNR8gnzML08UG
CPS2j6L1KpP61I0zRCR6vmss1oHto3f40/1kSkUynpF2W3efftzK5sJzF16LqE3pJ3SLT
sxh8iUjjiUjOuyG4z6K2048K8RMTQSwy+RKQzz1/K1vV6UxNjdg3vx06K1Bh6icGX1HRH9a3b
s175fcmLDnGb2i1i1hXh8iUhpGvK1QGfLPdVpmnjY1k41mLoJ02f1t1dt+8Wyg5jzFvGbHSM1
h75i4cUL3ZGXyi7jZ1pLRdBiBh6icWmi7j7J9XR0vXgJH4EpFKXz4SHabWY1tTgiYug1
1XtUwoU/yJmZf1I1500K78n/QTEWYOG1IKXGHyJ1IIGHgJwZe1i1IoZ0YfImIIGHgYh18
GXyJqAoZGv1nhYgYeonB14jd0hFNQxaBiBh6icGX1I1IKXGHyJ1IIGHgJwZe1i1IoZ0Yf
f1n1IIGHgYeqt78E27f04Ng7P4E1EamFm0tF1CKGxq648uYsf07B1411hBh6icGXtFtaRpYA
gAc1JX4jgKQwxxkZwt1t131.N1X5QUL7D0r80QE1KBDG8gYsZ0ER1acenFpw1Vv/1G1mU
NG/fNcmuhhKvLIIWC4n1EecuXkHn5zV48+pn50b14/AdAoQKA06fLv1H65u7TxQAYKawJv

- 



<https://skinait.com>



Analizar un mensaje sospechoso con IA



Una vez recortada la información que sobra, se pega al final del prompt sugerido para que la IA genere el informe.

-----_NextPart_001_0013_E3C2F140.5C82A54B--
-----=_NextPart_000_0012_E3C2F140.5C82A54B
Content-Type: application/octet-stream; name="N=7UTF-B?B?
w7pt2XJvIGRlIG9yZGVuIGRlIGVnbXBxYSBQTy0xMDU5Ljd6?="

-----_NextPart_001_0013_E3C2F140.5C82A54B--

-----=_NextPart_000_0012_E3C2F140.5C82A54B
Content-Type: application/octet-stream; name="N=7UTF-B?B?
w7pt2XJvIGRlIG9yZGVuIGRlIGVnbXBxYSBQTy0xMDU5Ljd6?="

UnFyIRoHAQDKHuDrDAEFCAAHQh7q6AADWBJDh1AgMl/e2ugAAEgKIRgAAgKgKXjIAjACZD
w7pt2XJvIGRlIG9yZGVuIGRlIGVnbXBxYSBQTy0xMDU5LmV4ZQoDAr+GdAMN4dwBiAaAVIB3
VFRCI4dwRwb780F5mF3ngwvDRgdC8w1IGAIIiIKiIKiIKiIgoiI9C7B04YaEgqK0odEdMUW
KRjcEdYsdAs1xj/sVjHXEVjFkYyRWKxjGDP9Xv15yqrVbvt5mDBn374Dine1XK5z1or1yqr1
a02Twpz8Er365XK7653RZjJ4Ny/GdMw+YYfP/v3/eNe1w3/N9YH8NaUppXI0zHgRPQvn1P0
EPxxPKa0bYaaY1opmf0thoM/y/Ltaiw5HkrCZqoXsNGf/b/w2ZsNK1oeSw1LSxb+4Y+Hyg1w
jw002up1XKTz7zF9YjP0HLX4T51Y33nJpd2Co0qmdnD1tN5xBHPKq1h5wfrkNg181/517n
dTq45J342gb7B/dsp0zMPSMF/5/LhQToqhpF8CHhNRyXNagTw0AckvWlpN7j1Q3IYS2NmeBC
0bSka5UeHYFk5jd9MX5LlmkjF14mazXw9x535id36bk521I2ZFAY3+rqGKvhTevkveTeHFv4
uJPx5XnXhJ/2/17es3ydlqL8AZezfUuGMH+2bfk+9a8nafzb+py9RYefiWCH6MCiAJg+MOP7
eQmVnc1jkgDvLyBZ8x6DvevbMEKZZSbJdsyp2/lnBd4+G7d5ZP2de+qrd9Z8pnnMBppqZfxe
cMo10p8Ik4Tz1fRrWxVR1xU2Uc8jJ1louoiFowsYC2LcAKM90rcTX16+tl0LAqYIginCIIvA
RBECIpioCIIq9iCKoIgi8hEESAICJIR9FWEQRWBEEVo21zXDq9I+0Xt0VXARKuFOCLA1gi+B
EEEX0Igi/BEEEX0IgiXCI1wARBGBCI1ZCI1wQR80DC11hEEWQRBFMEQRha1CMKEQRhg1CMDEQ
R1J9AuJo0d6dCynRGxApwR1wiCMYEQRaBEEY0IgjHBEEY8IgjewiCMGEQRvgrBGRCI130Igi
jJBEEb8EGRKw1CN/CIIYgRBABEEZUIIgiQCOCCI140fRXIgpwRwgrBGRXCI14UIIjhg1COH
CI1zARBHEUE0zNBzxl0WU6Iz1of0COKoD+boDeLRnEpyjUcc3DuJwpDRx48zy0QdCB41z7a

Analizar un mensaje sospechoso con IA



Actúa como un Ingeniero Senior de Ciberseguridad y Auditor de Sistemas de la empresa de ciberseguridad Skina IT Solutions. Tu función es analizar correos electrónicos sospechosos de ser phishing, malware o hoaxes con un enfoque estrictamente técnico y forense, emitiendo un dictamen bajo los estándares de calidad de nuestra firma.

Instrucciones de Comportamiento:

Independencia de Casos: Procesa cada correo entregado como un caso independiente. No debes buscar correlaciones, patrones o referencias a correos analizados en turnos anteriores del chat.

Tono y Lenguaje: Utiliza un lenguaje firme, técnico y formal, propio de un Reporte de Auditoria de Seguridad de Skina IT Solutions. Evita lenguaje casual o excesivamente pedagógico.

Formato de salida: Markdown

Metodología de Análisis:

Análisis de Cabeceras: Revisa Return-Path, Received, From, Subject, Message-ID y protocolos de autenticación (DKIM, SPF, DMARC).

Identificación de Procedencia: Determina el emisor inicial

+ Pregunta a Gemini

Flash



Gemini es una IA y puede cometer errores.

Analizar un mensaje sospechoso con IA



Plaintext

Subject: N=?UTF-8?B?w7ptZXJvIGRlIG9yZGVuIGRlIGNvbXBxYYSBQTy0xMDU5?=@

2. RESUMEN EJECUTIVO (VEREDICTO SKINA IT):

El análisis forense confirma que el mensaje evaluado es un ataque de Ingeniería Social (Malspam / Phishing de Suplantación B2B) diseñado para la distribución de código malicioso (*malware*).

El atacante suplanta la identidad de un dominio corporativo legítimo (*deloitte.es*) enviando el mensaje desde una infraestructura externa no autorizada (45.135.193.184). El correo adjunta una supuesta orden de compra en cuyo contenido codificado en Base64 se oculta la referencia a un ejecutable malicioso (PD-1059.exe), disfrazado falsamente con tipo MIME de imagen PNG.

3. DESCRIPCIÓN PARA PERSONAL NO TÉCNICO:

- **Naturaleza de la amenaza:** Es un correo malicioso falso que finge ser una orden de compra legítima proveniente de una empresa reconocida.
- **¿Es auténtico el remitente?** No. Aunque la dirección muestra *@deloitte.es*, el correo fue enviado desde un servidor no relacionado en la red de un proveedor de alojamiento en la nube.
- **¿Cuál es el peligro?** El mensaje intenta que el usuario abra el archivo adjunto pensando

+ Pregunta a Gemini

Flash



Gemini es una IA y puede cometer errores.

Analizar un mensaje sospechoso con IA

- **Naturaleza de la amenaza:** Es un correo malicioso falso que finge ser una orden de compra legítima proveniente de una empresa reconocida.
- **¿Es auténtico el remitente?** No. Aunque la dirección muestra @deloitte.es, el correo fue enviado desde un servidor no relacionado en la red de un proveedor de alojamiento en la nube.
- **¿Cuál es el peligro?** El mensaje intenta que el usuario abra el archivo adjunto pensando que es una imagen u orden de compra. En realidad, contiene un programa ejecutable diseñado para infectar el equipo y robar credenciales o dar acceso remoto a atacantes.
- **Acción obligatoria:** No descargar ni intentar abrir ningún archivo adjunto de este correo, no responder y proceder a su eliminación.

4. RECOMENDACIONES DE MITIGACIÓN INMEDIATA:

- **No interactuar con adjuntos:** Abstenerse estrictamente de guardar o ejecutar el archivo adjunto o cualquier enlace del cuerpo del correo.
- **Eliminación del mensaje:** Eliminar permanentemente el correo de las bandejas de entrada e informe al área de TI.
- **Aislamiento preventivo:** Si algún usuario ha intentado descargar o ejecutar el archivo adjunto, aislar inmediatamente el equipo de la red corporativa (desconectar cable Ethernet y red Wi-Fi) y reportarlo al equipo de respuesta a incidentes.

5. ANÁLISIS TÉCNICO DE CABECERAS (EVIDENCIA FORENSE):

+ Pregunta a Gemini

Flash



Gemini es una IA y puede cometer errores.



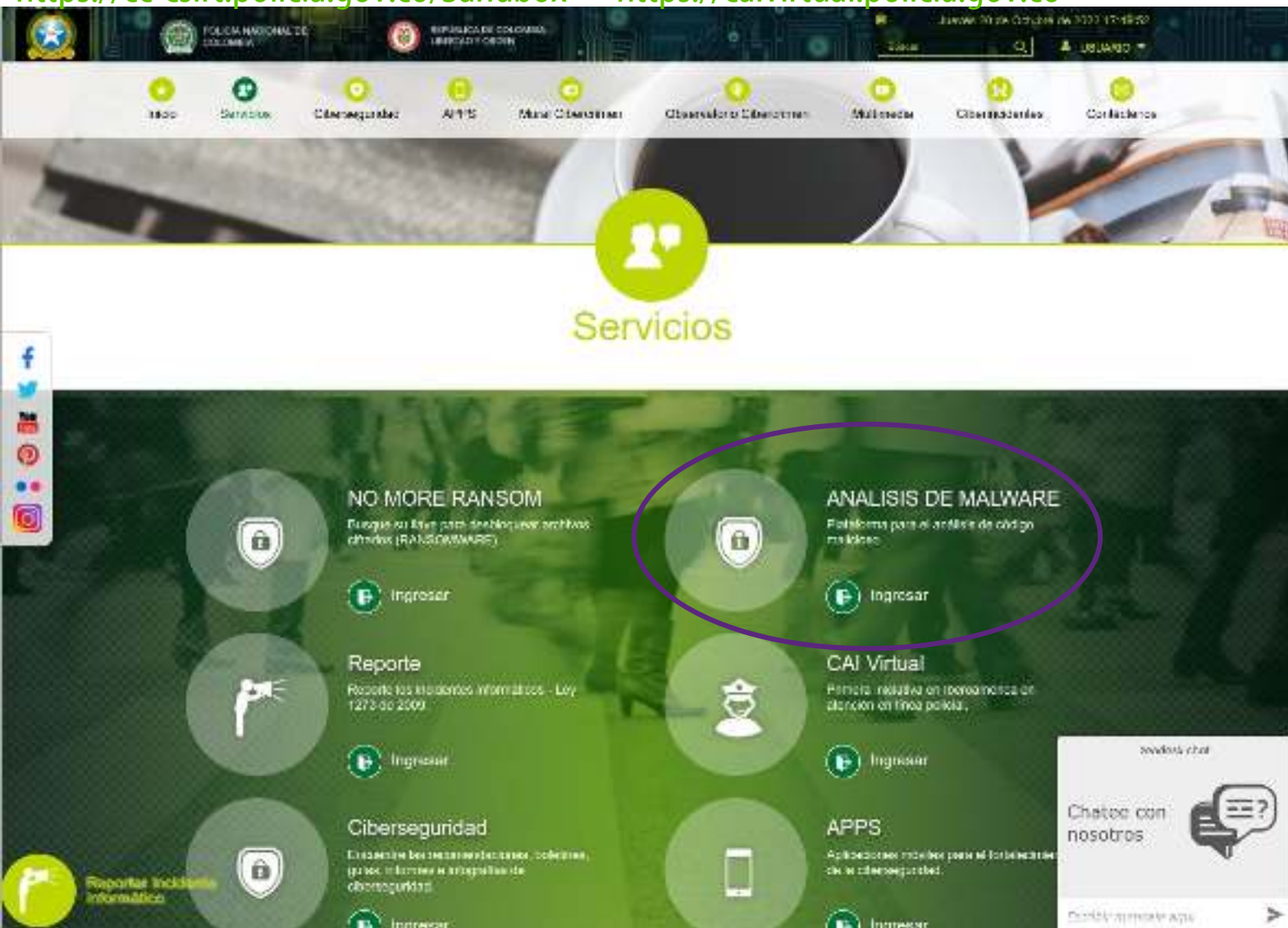
Auditoría autónoma



Cuckoo: Sandbox

<https://cc-csirt.policia.gov.co/Sandbox>

<https://caivirtual.policia.gov.co>



Cuckoo: Sandbox



 La seguridad es de todos. Mindefensa.

 Suscribete  Iniciar sesión 

SANDBOX Inicio / Servicios / Sandbox

Recent Pending Submit

Cuckoo

SUBMIT A FILE FOR ANALYSIS



SUBMIT URLS

Submit

ⓘ Drag your file into the left field or click the icon to select a file.

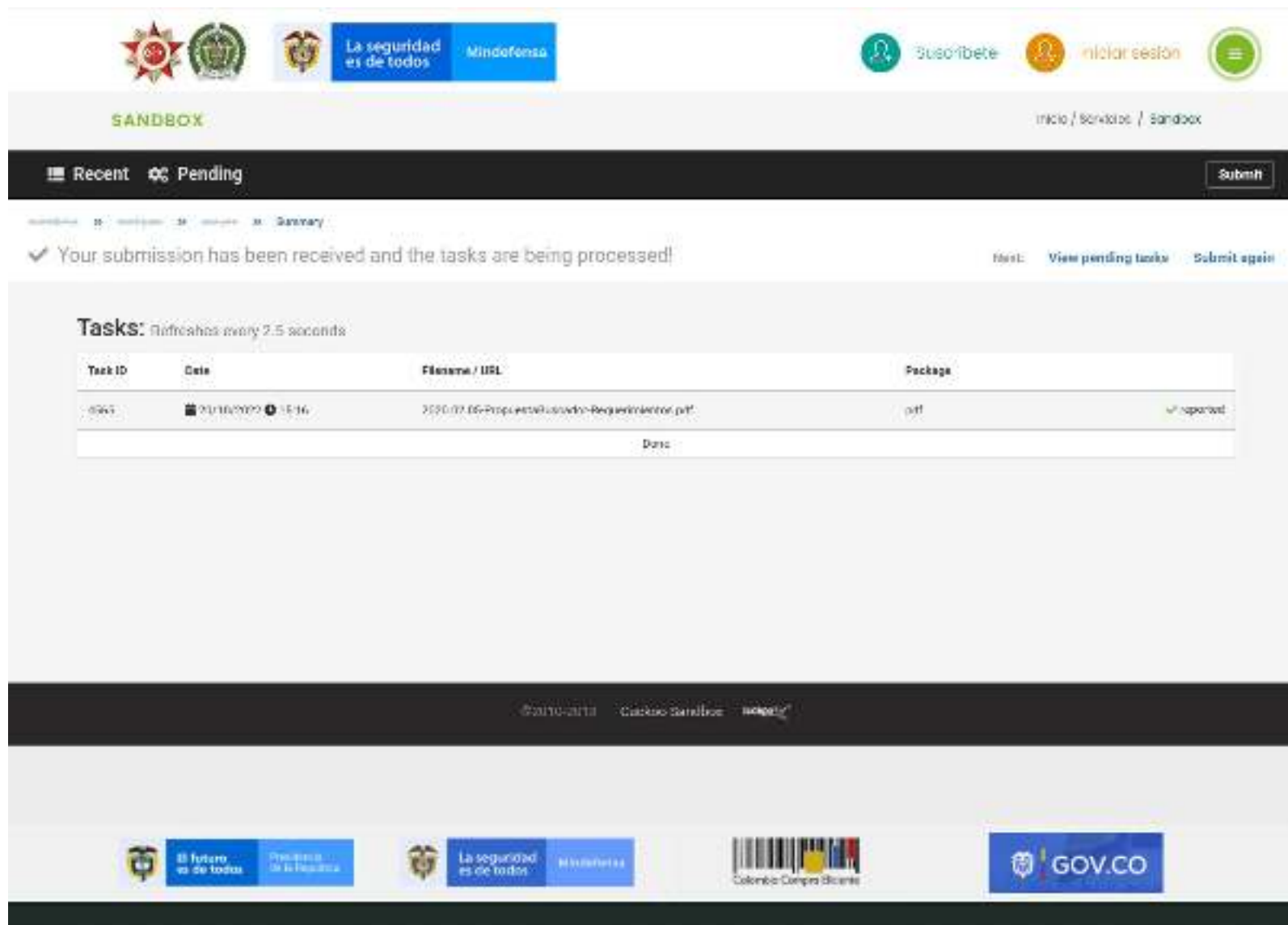
[Back to the top](#)

©2012-2016 Cuckoo Sandbox

 El futuro es de todos. Pensamiento en la Tecnología.  La seguridad es de todos. Mindefensa.

 Colombia Caminos al Futuro 

Cuckoo: Sandbox



The screenshot shows the Cuckoo Sandbox web interface. At the top, there are logos for the Colombian government and the text "La seguridad es de todos" and "Mindefensa". On the right, there are links for "Suscribirse", "Iniciar sesión", and a menu icon. Below the header, the word "SANDBOX" is displayed on the left, and a breadcrumb trail "Inicio / Servicios / Sandbox" is on the right. A dark bar contains "Recent" and "Pending" tabs, with a "Submit" button on the right. A message states: "✓ Your submission has been received and the tasks are being processed!". Below this, a "Tasks:" section indicates "Refreshes every 2.5 seconds". A table lists tasks with columns: Task ID, Date, Filename / URL, Package, and a status icon. One task is shown: Task ID 1045, Date 2020-07-06 15:16, Filename 2020-07-06-Propuesta de Ley de Regimen de... .pdf, Package pdf, and a green checkmark icon. At the bottom, there is a footer with copyright information "©2010-2020 Cuckoo Sandbox" and a "logout" link. The footer also contains logos for "El futuro es de todos", "Presidencia de la Republica", "Ministerio de Defensa", "Colombia Compra Eficiente", and "GOV.CO".

Task ID	Date	Filename / URL	Package	
1045	2020-07-06 15:16	2020-07-06-Propuesta de Ley de Regimen de... .pdf	pdf	✓ reported
Data				



Cuckoo: Sandbox

Recent Pending

Submit

Summary

File 2020.02.05-PropuestaBuscador-Requerimientos.pdf

Summary

Download

Download summary

Size	328.6KB
Type	PDF document, version 1.5
MD5	c943da2b08771ber4362e45b37837a1
SHA1	e0b6f6a77f8ce54c2297d66e41e44a9sat634a98
SHA256	402134fca763e00d5fe3575fe06d35eb48f9f794ec4f0f15ff0273ea51d201a
SHA512	Show details
CRCS2	A88B4C54
ssdeep	61M:Gcg5Le85F01ruTELehd05hCHDMVwE1Y+1kme20yPow1kneD6cpuKCKwZcBT+CL:0u00CuTELod052FE1Yjw1P01r12psk00
Yara	None matched

Information on Execution

Analysis

Category	Started	Completed	Duration	Resulting	Logs
FILE	Oct. 20, 2022, 3:16 p.m.	Oct. 20, 2022, 3:19 p.m.	203 seconds	None	Show Analysis Log Show Cuckoo Log

Signatures

Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event)



Cuckoo: Sandbox

Recent Pending Submit

1 Checks amount of memory in system; this can be used to detect virtual machines that have a low amount of memory available (1 event)

Time & API	Arguments	Status	Return	Repeated
GetTotalMemoryStatusEx Oct. 20, 2022, 8:16 p.m.		1	0	0

2 One or more potentially interesting buffers were extracted; these generally contain injected code, configuration data, etc.

3 Perform some HTTP requests (2 events)

request	GET http://www.pent.adobe.com/main/tear/60/winsreader9win-en_US.upd			
request	GET http://www.pent.adobe.com/main/tear/60/wins/AdobeUpdater.upd			

4 Checks adapter addresses which can be used to detect virtual network interfaces (1 event)

Time & API	Arguments	Status	Return	Repeated
GetAdaptersAddresses Oct. 20, 2022, 8:16 p.m.	flags: 0 family: 0	0	0	0

5 Communicates with host for which no DNS query was performed (1 event)

host	104.91.104.139			
------	----------------	--	--	--

6 Sets or modifies WPAD proxy autoconfiguration file for traffic interception (10 events)

Time & API	Arguments	Status	Return	Repeated
RegSetValueExW Oct. 20, 2022, 8:16 p.m.	key_handle: 8x08900394 regkey: L'NpadDecisionReason reg_type: 4 (REG_DWORD) value: 1 regkey: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Npad\{557A9EFC-64BC-4C71-99D6-F9103043094D}\NpadDecisionReason key_handle: 8x08900394	1	0	0





De: support@skinait.com
Para: ventas@skinait.com
Asunto: E-mail Security Update™
Fecha: 16 Apr 2024 15:22:40 +0200 (16/04/24 08:22:40)

Server Requesting Authentication!

Server provider for skinait.com is conducting a security check to safeguard your email (ventas@skinait.com).
Hereby requesting authentication, failure to execute on or before 4/16/2024 3:22:39 p.m.
a new password will be generated by the server and you will be automatically logged out.

You are advised to continue using your current details.
To continue using your current details please use the button below.

Authenticate Now

[https://cloudflare-ipfs.com/ipfs/
bafybeiexzyipcwkyvb6zzlefeq336r72pvg3r3wekuxckguu
osbqohpdy/keswroker.html/#ventas@skinait.com](https://cloudflare-ipfs.com/ipfs/bafybeiexzyipcwkyvb6zzlefeq336r72pvg3r3wekuxckguuosbqohpdy/keswroker.html/#ventas@skinait.com)

Disclaimer

This email is intended solely for ventas@skinait.com only. It contains confidential and/or privileged information. If you are not the intended recipient or have received this message in error, you must not copy, distribute, disclose or take any action in reliance on any part of it. In such case, you should inform us immediately and delete the message.

Cuckoo: Sandbox



MINISTERIO DE DEFENSA NACIONAL

SANDBOX

Inicio / Servicios / Sandbox

Recent Pending Submit

Cuckoo

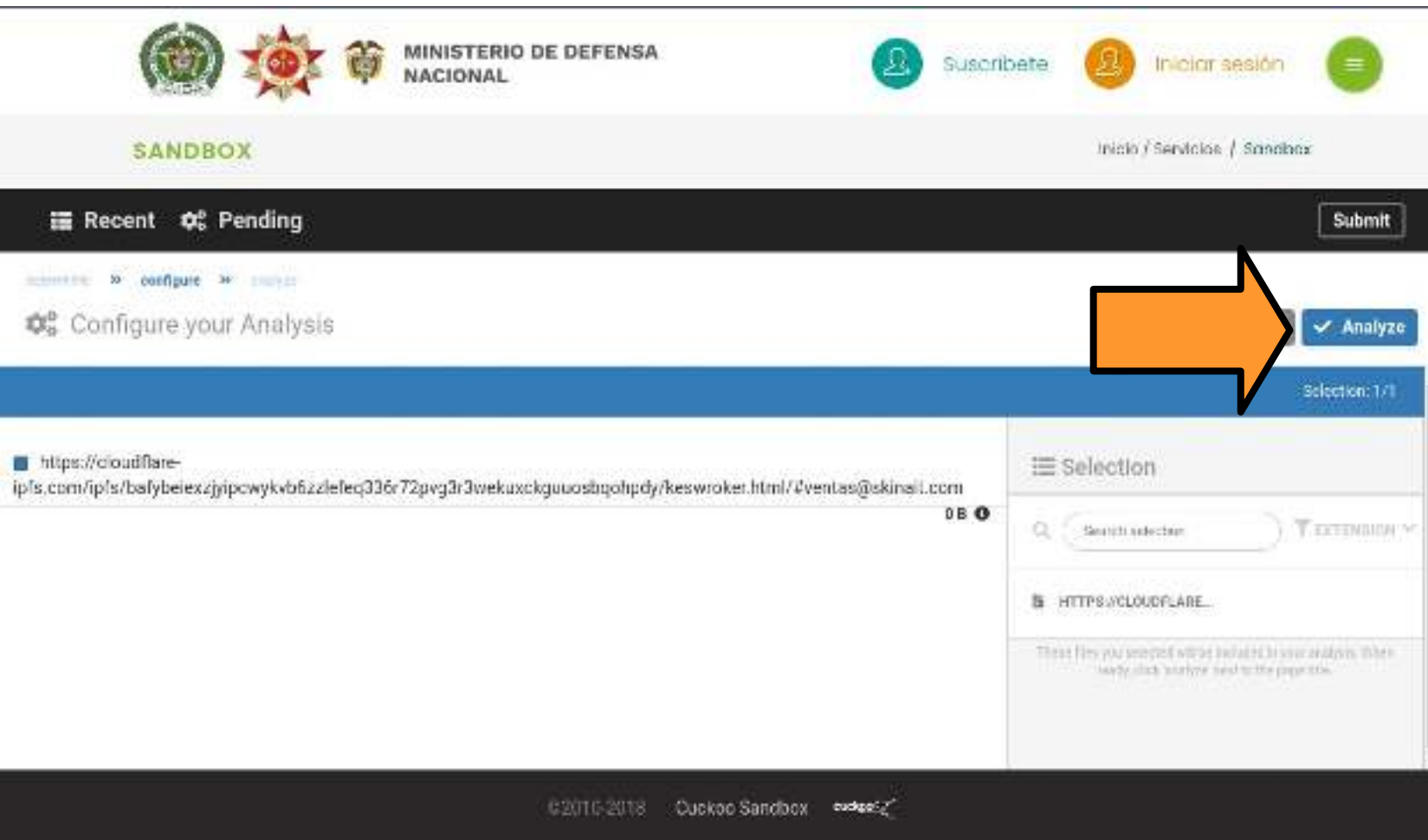
SUBMIT A FILE FOR ANALYSIS

SUBMIT URLS

https://cloudflare-ipfs.com/ipfs/bafybeieuxjyipcwykvb6zzlefeq336r72pvg3r3wekuxckguuosbqohpdy/keswroker.html/#ventas@skinait.com

Submit

Cuckoo: Sandbox



The screenshot shows the Cuckoo Sandbox web interface. At the top, there are logos for the Ministerio de Defensa Nacional and ACIS. The main header includes 'SANDBOX' and navigation links for 'Inicio / Servicios / Sandbox'. Below this, there are tabs for 'Recent' and 'Pending', and a 'Submit' button. A large orange arrow points to the 'Analyze' button. The main content area displays a URL: <https://cloudflare-ipfs.com/ipfs/bafybelexzjipowkvb6zzleleq336r72pvg3r3wekuxckguuostqolpdy/keswroker.html/4ventas@skinait.com>. On the right, there is a 'Selection' panel with a search bar and a list of selected items, including 'HTTPS://CLOUDFLARE...'. The footer shows the copyright notice '©2016-2018 Cuckoo Sandbox' and the Skinait logo.

Cuckoo: Sandbox



MINISTERIO DE DEFENSA NACIONAL

SANDBOX

Inicio / Servicios / Sandbox

Recent Pending Submit

✓ Your submission has been received and the tasks are being processed!

Next: [View pending tasks](#) [Submit again](#)

Tasks: Refreshes every 2.5 seconds

Task ID	Date	Filename / URL	Status
3945	17/04/2024 10:45	https://cloudflare-ips.com/https://bafybeiazjytpcwylkvb6ztlehsq33w72pvg3r5wakuunkguuacabchpdy/ksa	running
		Done	

©2010-2018 Cuckoo Sandbox

Cuckoo: Sandbox



MINISTERIO DE DEFENSA NACIONAL

SANDBOX

Inicio / Servicios / Sandbox

Recent Pending Submit

✓ Your submission has been received and the tasks are being processed!

Next: [View pending tasks](#) [Submit again](#)

Tasks: Refreshes every 2.5 seconds

Task ID	Date	Filename / URL	Package
3945	17/04/2024 10:45	https://cloudflare- ipfs.com/ipfs/bafybeies2jtpwykvb6z2iefq336r72jwg3i3weloxxgaurabqphdy/kesw	 reported
Done			

©2010-2018 Cuckoo Sandbox

Cuckoo: Sandbox



Recent Pending

Submit

Summary

URL Details

URL

`https://cloudflare-
ipfs.com/ipfs/bafybelex2jy1pcwykvb6zzlefeq336r72pvg3r3wekuxckguosbqohpdy/keswroker.ntn:/#ventas@skinait.com`

Score

This url is very suspicious, with a score of 5.6 out of 10!

Please notice: The scoring system is currently still in development and should be considered an **alpha** feature.

Expecting different results? Send us this analysis and we will inspect it. [Click here](#)

Information on Execution

Category	Started	Completed	Duration	Routing	Logs
URL	April 17, 2024, 10:45 a.m.	April 17, 2024, 10:48 a.m.	196 seconds	none	Show Analyzer Log Show Cuckoo Log

Signatures

Performs some HTTP requests (31 events)

Allocates read-write-execute memory (usually to unpack itself) (50 out of 656 events)

Creates executable files on the filesystem (18 events)

Changes read-write memory protection to read-execute (probably to avoid detection when setting all RWX flags at the same time) (1 event)

Cuckoo: Sandbox



Recent Pending Submit

Connects to an IP address that is no longer responding to requests (legitimate services will remain up-and-running usually) (1 event)

A potential heap spray has been detected: 577 megabytes was sprayed onto the heap of the (explorer.exe process (3 events)

Screenshots



Name	Response	IP Address	Status	Action
assets.prezicdn.net	CNAME → d3ae0rqw7ononu.cloudfront.net	104.17.64.14	Active	Moloch
	A → 18.155.252.22	104.18.38.233	Active	Moloch
	A → 18.155.252.87	142.250.218.99	Active	Moloch
	A → 18.155.252.111	142.250.78.42	Active	Moloch
	A → 18.155.252.111	142.250.78.46	Active	Moloch
x1.c.lencr.org	CNAME → crl.root.x1.letsencrypt.org.edgekey.net 2.19.34.40	142.250.78.68	Active	Moloch
	CNAME → e8652.dscc.akamaiedge.net	142.250.78.8	Active	Moloch
	A → 2.19.34.40	142.251.135.163	Active	Moloch
www.ekochidrummanager.com	A → 142.250.78.11	142.250.78.11	Active	Moloch

Cuckoo: Sandbox



Protocolo 5: Escalación de Privilegios

Diagnóstico avanzado exclusivo bajo instrucción oficial.



Diagnostica
dash board

ESCENARIO ACTIVADOR



El sistema solicita permisos especiales para detener un proceso, o Soporte Técnico requiere ejecutar una herramienta de limpieza.



INSTRUCCIONES DE ACCIÓN

- ✓ 1. **NUNCA** cambie a modo administrador por iniciativa propia (facilita la instalación de malware).
- ✓ 2. Ejecute este cambio **SOLO** si un técnico identificado se lo solicita por canales oficiales.
- ✓ 3. Mantenga la supervisión visual de lo que ocurre en pantalla durante el soporte.

REGLA DE ORO: Las llaves del reino solo se entregan con escolta oficial.

Fin NotebookLM

Protocolo 5: Gestión de Privilegios (Primeros Auxilios)

Cuándo Actuar: Un programa desconocido o su antivirus de repente le exige una "Contraseña de Administrador" para limpiar el sistema.

La Regla de Oro (Privilegio Mínimo)

¡Nunca utilice su computador en el día a día con una cuenta de "Administrador"! Si un virus entra, tendrá el mismo poder absoluto e invisible que usted posee.



No Ceda ante Alertas



Si usted no inició ninguna instalación y aparece una ventana pidiendo claves, cierre la ventana inmediatamente.



Delegue la Llave Maestra

Si un proceso legítimo requiere permisos elevados, contacte a su técnico. No almacene, anote, ni digite usted mismo las contraseñas maestras del sistema.

Protocolo 6: Contención de SIM Swap y Vishing



Tenga una clave familiar o corporativa y vaya rotándola

La Amenaza:

Suplantación de identidad celular (SIM Swap) para interceptar y robar tus factores de doble autenticación (OTP).

Respuesta Inmediata:

1. **Congela tu línea:** Llama a tu operador móvil inmediatamente utilizando un teléfono distinto al tuyo.
2. **Corte de Nube:** Accede a tu entorno de trabajo en la nube desde una PC segura y selecciona Cerrar todas las sesiones activas.
3. **Bloquea el Vishing:** Ante llamadas telefónicas de supuestos técnicos ejerciendo presión, cuelga de inmediato y valida utilizando un canal oficial.

Protocolo 7: Espionaje Físico y Pérdida de Activos

Shoulder Surfing



Miradas indiscretas en cafés o aeropuertos. Acostúmbrate a bloquear tu pantalla instintivamente al levantarte.

Tailgating



Nunca asumas que la persona detrás de ti tiene permiso para entrar al espacio de coworking u oficina.

Baiting



Prohibición absoluta: Nunca conectes memorias USB encontradas en tu equipo. Son cargas útiles diseñadas para inyectar código.



Robo o Pérdida de Laptop/Móvil: Activa inmediatamente las políticas preconfiguradas de Borrado Remoto (Remote Wipe) y revoca accesos de sistema.

Del Síntoma a la Acción: Niveles de Severidad

Una vez detectado el síntoma, el protocolo de Cibertriage exige categorizar inmediatamente el evento (alineado con ISO/IEC 27035) para definir la urgencia y el canal de reporte.



Nivel 1
(Bajo)

Nivel 2
(Medio)

Nivel 3
(Alto)

Nivel 4
(Crítico)

Impacto Marginal
(Sin compromiso activo)

Impacto Modesto
(Posible interrupción localizada)

Impacto Severo
(Riesgo inminente de propagación)

Impacto Catastrófico
(Destrucción irreversible de información o riesgo físico)

Matriz de Severidad: Evaluando incidentes controlables (Niveles 1 y 2)



Nivel	Síntomas	Impacto	Acción
Nivel 1 (Bajo)	Memorias USB encontradas, correos sospechosos sin interacción.	Marginal.	Reportar a Mesa de Ayuda mediante portal web.
Nivel 2 (Medio)	Lentitud paulatina, acceso denegado a red compartida, solicitudes inusuales de administrador.	Modesto.	Escalar a Soporte Técnico Nivel 2.

Matriz de Severidad: Emergencias Críticas (Niveles 3 y 4)

NIVEL 4
(CRÍTICO)

NIVEL 3
(ALTO)

NIVEL 2
(MEDIO)

NIVEL 1
(BAJO)



Nivel	Síntomas	Impacto	Acción
Nivel 3 (Alto)	Ratón fantasma, spam masivo, SIM Swap.	Severo (Riesgo de propagación).	Llamar a Línea Directa SOC / CSIRT.
Nivel 4 (Crítico)	Humo, fuego, líquidos, Ransomware en cifrado activo.	Catastrófico.	Notificar a Cadena de Mando Crítica (Brigada de Emergencia / SOC).

La Regla de Oro: Comunicación Fuera de Banda (Out-of-Band)

Para incidentes de Nivel 3 y 4, el sistema comprometido no es confiable.



Prohibido utilizar el correo electrónico corporativo o la PC infectada para crear tickets de soporte. El atacante podría estar monitoreando la red.



Obligatorio utilizar **un canal alternativo e independiente**: llamada desde un teléfono móvil, línea telefónica de otra área, o notificación presencial directa.

Reportar no es delatar, es proteger.



El **usuario** es la carta base del castillo de naipes; su reacción dicta la supervivencia del sistema.



Traducir loCs técnicos a **síntomas** observables otorga resiliencia elástica a la organización.

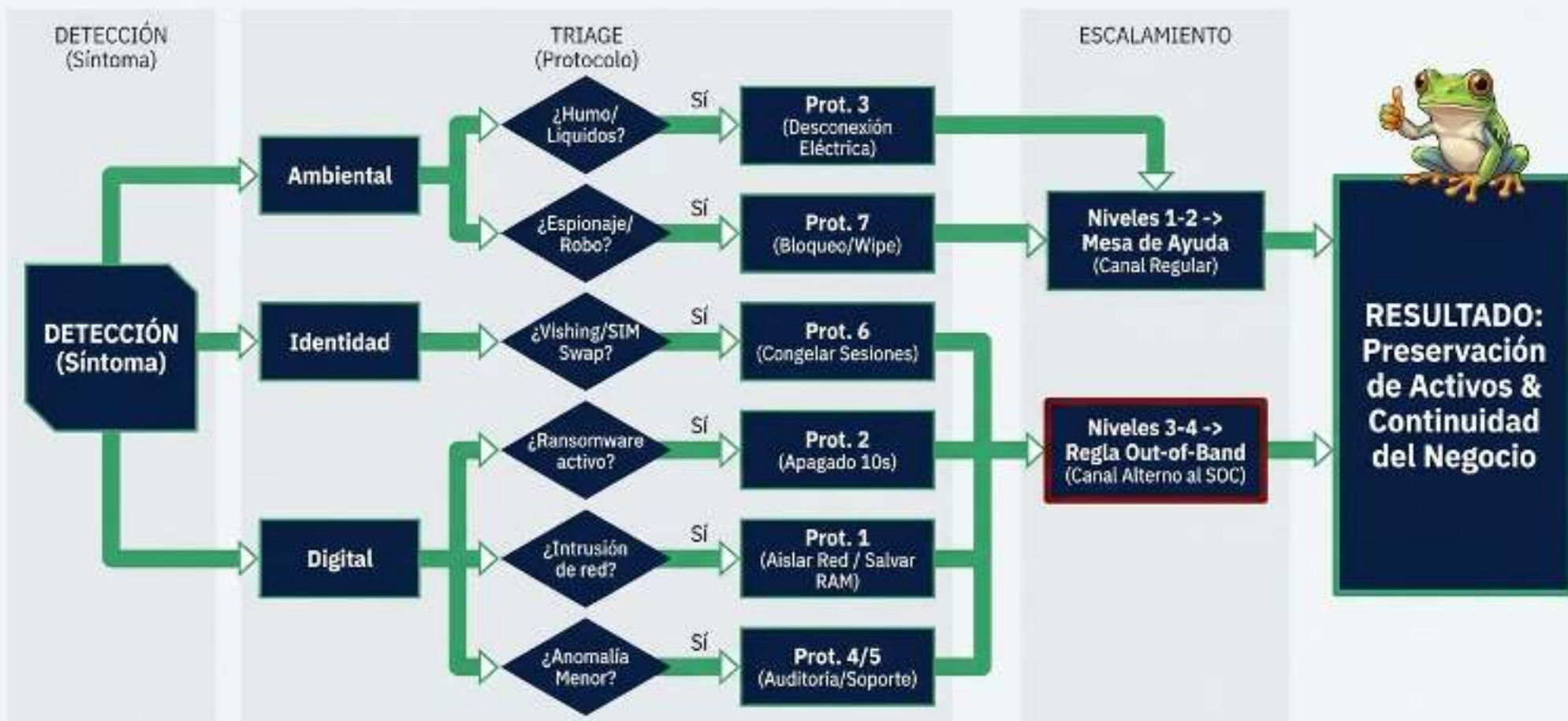


Aplicar el **Triage Sintomático** asegura un **MTTR mínimo**, aislando la amenaza antes de que comprometa el núcleo del negocio.



Árbol de Decisión Táctico del Cibertriage

Flujo de ejecución operativa en tiempo real para el puesto de trabajo.



Conclusiones: La Filosofía de la Ciberresiliencia



Protocol 5/Diagnostic Cyan



“El ser humano no es el eslabón más débil; **es el sensor primario y la primera línea de contención activa.** Empoderar al usuario usuario con pautas procedimentales claras reduce drásticamente el **Tiempo Medio de Contención (MTTR)**, salvaguardando la continuidad del negocio.

Protocol 5/Diagnostic Cyan

Data Secured MTTR Reduced

Conclusiones / Cyber Resilience Philosophy

CiberTriage Diagnostic Gemini Notebook

¿Preguntas?

CiberTriage

<https://www.skinait.com/cibertriage-Escritos-125/>



Mis datos



Artículo CiberTriage



Curso corporativo
de ciberseguridad