TRABAJO DE GRADO
Opción Seminario-Diplomado.

Propuesta de endurecimiento tecnológico para aprendamos Ltda. Mediante el despliegue de la herramienta de honeypots T-pot

Corporación Universitaria Remington.

Nombre de la facultad: Ingenierías

Realizado por:

Marlon Stiven Cordoba Palacios

Ronald Fabián Caro Parra

Tutor:

Iin. Esp. ALFONSO VALENCIA Msc

Septiembre, 2026

Valledupar – Colombia

Tabla de contenido

Resumen 3
Marco conceptual 4
Marco contextual 6
Visión 8
Estructura Organizacional 8
Objetivo General 8
Objetivo Específicos 9
Marco conceptual ..... **¡Error! Marcador no definido.**
Herramientas de Análisis y Visualización ..... **¡Error! Marcador no definido.**
Marco Referencial ..... **¡Error! Marcador no definido.**
Problemática Empresarial 10
Justificación Práctica y de Negocio 10
Plan de respuesta a incidentes 11
Adaptacion del plan al Router Sagemcon CS50001 13
Politica de contraseñas seguras – Aprendamos Ltda 15
Vigencia y rotación 15
Gestión y custodia de credenciales 15
Implementación técnica inmediata 16
Guía de configuración técnica de T-Pot 16
Descarga e instalación del T-Pot 16
Reasignación de puerto 17
Acceso al panel de control 17
Conclusión 18
Referencias 19

Resumen

En este trabajo se propone un esquema de endurecimiento tecnológico para el Centro de Enseñanza Automovilística Aprendamos Ltda. en Valledupar, cuya operación depende críticamente de la conectividad para el registro y validación ante el Registro Único Nacional de Tránsito (RUNT).

El objetivo principal consiste en fortalecer la detección de amenazas mediante la implementación de la plataforma de código abierto T-POT. La metodología se estructura en cuatro fases consecutivas: el análisis de activos, el diseño de una arquitectura basada en señuelos, el establecimiento de una red administrativa y el despliegue de la solución sobre un ordenador reutilizado con el sistema operativo Debian 12. Dentro del entorno de T-POT, se incorporan los honeypots Cowrie y Dionaea para la recolección y análisis de malware..

Como resultado del proyecto, se genera un plan de respuesta a incidentes fundamentado en la guía NIST SP 800-61, una política de seguridad para contraseñas alineada con el estándar NIST SP 800-63B y un informe técnico que incluye una lista de verificación semanal de 15 minutos optimizada para la plataforma Kibana.

Palabras clave

Honeypot, T-Pot, Debian, Kibana, Cowrie, Dionae, Kibana, Endurecimiento tecnológico, Respuesta a incidentes, Análisis de activos, Red administrativa, NIST SP 800-61, NIST SP 800-63B, NIST, RUNT, Ley 1581 de 2012, Resolución 0809 de 2014

Marco conceptual

Honeypot: "Señuelo sin valor operativo donde toda interacción con este se puede decir que es maliciosa" (Spitzner, 2003).

Inteligencia de amenazas: “Conocimiento basado en evidencia sobre tácticas para anticipar diferentes tipos de ataques” (MITRE, 2024).

Superficie de exposición: "La suma de puntos vulnerables donde un actor no autorizado puede intentar introducir o extraer datos de una red; en la academia incluye terminales biométricos, equipos administrativos y dispositivos móviles conectados al Wi-Fi" (INCIBE-CERT, 2023).

Movimiento lateral: "es el desplazamiento del atacante desde el señuelo hacia el servidor real (esto sería una alerta de gravedad alta)" (MITRE, 2024).

Tecnologías de engaño y Honeypots: "Un honeypot es un recurso informático de seguridad diseñado para ser atacado o comprometido; al no tener valor operativo, toda interacción con este se considera sospechosa" (Spitzner, 2003; Provos y Holz, 2007; INCIBE-CERT, 2003).

Clasificación según su nivel de interacción

Baja interacción: "Simulan servicios básicos, consumen poco recurso y reducen el riesgo de pivote, aunque recolectan información limitada" (INCIBE-CERT, 2023).

Alta interacción: "Ejecutan sistemas o servicios reales o completos permiten observar tácticas comandos y malware a costa de mayor riesgo y consumo" (INCIBE-CERT, 2023).

El ecosistema T-Pot

"T-pot es una plataforma de código abierto desarrollada por Deutsche Telekom Security que centraliza múltiples hoynepots en contenedores Docker sobre un único equipo físico o virtual" (Deutsche Telekom Security, 2024). Para este proyecto resultan necesarios:

- **Cowrie: "**honeypot de mediana a alta interacción que emula SSH y Telnet registra fuerza bruta, credenciales y muestras en entorno aislado" (Oosterhof, 2024).
- **Dionaea:** "emula SMB, HTTP, FTP y TFTP para lograr capturar exploits y malware automatizado" (Dionaea Project, 2023).
- **Honeytrap**: "son sensores dinámicos que analizan los puertos no cubiertos y permite identificar barridos y vulnerabilidades desconocidas" (Werner, 2023).

Herramientas de Análisis y Visualización

“T-Pot centraliza la telemetría para su interpretación visual por el administrador” (Elastic, 2024ª, 2024b)

- **Elasticsearch: “**motor distribuido de búsqueda y analítica que indexa registros, IP y comandos de cada honeypot” (Elastic, 2024a).
- **Kibana**: “interfaz que permite tableros en tiempo real con geolocalización mostrando los puertos más atacados y las credenciales observadas” (Elastic, 2024a).
- **Logstash / Filebeat**: herramientas de recolección, procesamiento y normalización de registro Docker antes de su almacenamiento

"El uso de honeypots tránsito de proyectos académicos como The Honeynet Project a inicios de los 2000 a su integración en centros de operaciones de seguridad como parte de tecnologías reconocidas en el marco MITRE ATT y CK" (Spitzner, 2003, MITRE, 2024, Strom et al. 2020).

Marco contextual

“El centro de Enseñanza Automovilística Aprendamos Ltda fundado en 1990 en Valledupar ofrece formación en conducción motos, carros, camiones y programas técnicos en tránsito” (Aprendamos Ltda s.f EMIS, 2026).

Opera bajo resolución 0809 de 2014 del ministerio de transporte con 24 vehículos inscritos y estructura de gerencia, coordinación académica y de calidad baso ISO 9001 2015.

Tabla 1

Dato legal	**Registro**
Dato legal	**Registro**
	Aprendamos Ltda.
Razón social	Centro de Enseñanza Automovilística N.° 13B-36, Valledupar
Dirección	Carrera 9 N.° 13B-36, Valledupar
Teléfono	5807576 / 3163827209
Registro mercantil	33548
NIT	800.170.208-5
Representante legal	Lenis Catherine Escamilla de la Cruz
Cedula representante legal	55.221.473
Inscripción ministerio de transporte	Resoluciones 0009242 – 000830 - 000809
Vehículos inscritos	

Nota. Esta tabla fue elaborada a partir de documentación aportada por la empresa

En los siguientes apartados se dará más información sobre la empresa para contextualizar más la redacción.

Misión

“somos una empresa de carácter privado que brinda los servicios de enseñanza automovilística para conductores en las categorías motos, carros y camiones a clientes particulares e institucionales garantizando amabilidad y puntualidad en el servicio tenemos horarias flexibles, facilidades de pago y renovación del parque automotor”.

Visión

"En el año 2030 consolidarnos como el centro de enseñanza automovilística numero uno a nivel regional, fundamentando las buenas acciones pedagógicas y teniendo un buen modelo de gestión de calidad".

Estructura Organizacional

La organización está definida por líneas de mando y niveles jerárquicos (Gerencia, Coordinación, secretaria, Instructor y Contador) cada uno con sus responsabilidades descritas en los manuales de funciones. La gerencia se encarga de ordenar al coordinador para asegurar la continuidad del sistema integrado de gestión.

Objetivo General

Proponer un esquema de endurecimiento tecnológico para Aprendamos Ltda. mediante el análisis, despliegue de la plataforma de honeypot con la herramienta de código abierto T-Pot con el fin de fortalecer la detección de amenazas y posturas de seguridad en el entorno corporativo.

Objetivo Específicos

Analizar la documentación de la infraestructura y flujo de datos de Aprendamos Ltda, con esto se identificará los activos críticos y vectores mediante una visita técnica, se hará una revisión del PEI y la matriz de riesgos, sin hacer alguna interversion sobre producción.

Diseñar a nivel lógico la arquitectura de despliegue de T-Pot, definiendo la ubicación de los señuelos, la segmentación administrativa y adaptar la matriz de contención al Sagemcom CS50001.

Formular el procedimiento teórico de la configuración del T-Pot a partir de la documentación oficial la cual será validada mediante lista de chequeos y diagramas.

Elaborar una guía teórica de mitigación con IRP (Plan de Respuesta a Incidentes) basado en NIST SP 800-61 y se harán chequeos semanales.

Problemática Empresarial

Aprendamos Ltda ha digitalizado procesos misionales dependientes de conectividad como el registro biométrico y la validación de certificados ante autoridades de transito el flujo de usuarios externos en redes locales y el tratamiento de datos sensibles amplían la superficie de exposición un incidente paralizaría la operación y generaría sanciones y perdida de confianza. Ante presupuestos limitados se requiere una estrategia proactiva de bajo costo basada en T-Pot para desviar, analizar y contener ataques sin comprometer la viabilidad financiera.

Justificación Práctica y de Negocio

En Colombia la validación biométrica y el cargue al RUNT exigen conectividad estable un ataque ransomware interrumpiría clases y congelaría ingresos asimismo la custodia de huellas, identificaciones y transacciones obliga al cumplimiento de la ley 1581 de 2012, cuya infracción sanciona la superintendencia de industria y comercio.

Impacto financiero: un ataque paralizaría clases teóricas y practicas con perdida diaria por alumno no registrado.

Reputación y legalidad: la filtración dañaría la confianza y acarrearía sanciones por violación de datos personales. El proyecto mitiga estos riesgos de forma continua y precisa.

Para Aprendamos Ltda. el plan de respuesta a incidente (IRP) debe ser ágil, de bajo costo y orientado a proteger la validación biométrica, seguimiento la guía NIST SP 800-61 Rev.2 (Cichonski et al, 2012).

Plan de respuesta a incidentes

A continuación, se presenta el IRP ante las alertas de T-Pot estructurado según Cichonski et al (2012).

1. **Preparación (antes del incidente)**

   Esta fase asegura la capacidad de actuación previa al ataque se recomienda ubicar el T-Pot en VLAN aislada y separar la red de invitados y la red administrativa mediante contrafuegos. Se tienen que configurar las alertas en Kibana por correo o telegram ante picos de fuerza bruta y se tiene que mantener el inventario actualizado de las IP y los equipos administrativos para determinar el origen interno o externo.

2. **Detección y análisis**

   El honeypot opera como una alerta temprana. Flujo de red general el actor externo escanea e interactúa con el T-Pot y se genera la alerta en Kibana y se identifica el

IP. Se clasifican como gravedad alta si se observan intentos de movimientos latelares hacia el servidor real.

Tabla 2

Escenario detectado en T-Pot	**Acción de contención**	**Erradicación y recuperación**
Escenario detectado en T-Pot-Fi de los alumnos	**Acción de contención**reouter/AP y bloquear el acceso inalámbrico inmediato	**Erradicación y recuperación**
Ataque desde Wi-Fi de los alumnos	Localizar IP/MAC en el reouter/AP y bloquear el acceso inalámbrico inmediato	Forzar el cambio de clave de invitados si el ataque fue masivoMalwarebytes/Kaspersky y limpiar persistencias antes de reintegro
Ataque desde red administrativa	Desconectar o asilar el quipo la operación continua desde otros equipos	Analizar con Malwarebytes/Kaspersky y limpiar persistencias antes de reintegro
Ataque de IP pública externa		

Tabla elaborada con información basada en Cichonski et al. (2012).

3. Actividades Post-Incidente

Se realiza reunión de cierre para determina los vectores de ingreso y hacer ajustes de recursos en caso de saturación y actualización de segmentación y privilegios.

Adaptación del plan al Router Sagemcon CS50001

En visita técnica se documentó router sagemcom CS50001 y switch de 24 puertos TP-Link TL-SG1024 no administrable al no disponer de CLI empresarial, la contención se ejecuta via interfaz web, lo cual resulta viable en PYME colombianas por su bajo costo, aunque impone restricciones de segmentación avanzada.

Fase de preparación: se tiene que acceder a 192.168.0.1 o 192.168.100.1 luego pestaña Wireless > Guest Network, creación de red exclusiva para alumno y la activación de insólate clientes / AP Isolation para impedir comunicación lateral hacia la red administrativa y la conexión con el T-Pot va via cable LAN principal.

Fase de detección: la alerta de Kibana provee IP y MAC de origen

Contenido A – filtro MAC (Wi-Fi): Wireless > Access control en modo Deny list, registro de MAC reportada y aplicación para expulsión inmediata.

Contencion B – filtro IP (red cableada): Advanced > IP filtering, regla de denegación hacia segmento biometrico mientras se desconecta físicamente el equipo.

Erradicación: rotación de credenciales si hubo éxito parcial en el señuelo y auditoria en Advanced > Port forwarding para cerrar la exposición innecesaria.

A continuación, se indica las credenciales genéricas por defecto y el procesamiento inmediato para cambiarlas.

Las credenciales por defecto del Sagemcom CS50001 se observa en la siguiente foto.

Foto 1



Etiqueta física del router Sagemcom CS50001 (F@st 3686 V2) documentado en visita técnica fotografía propia (2026). Los seriales son visibles solo con fines académicos en la versión públicas se difumina según la ley 1581 de 2012 (congreso de Colombia, 2012)

El proveedor de internet asociado al equipo documento es claro Colombia

El acceso por defecto observado es la siguiente combinación

Usuario: admon.

Contraseña: admin

Politica de contraseñas seguras – Aprendamos Ltda

Diseñada según Grassi et al. (2017) (NIST SP 800-63B).

1. **Longitud y complejidad**

   Se prohíbe el uso de claves cortas tradicionales se adoptan frases de contraseñas de mínimo 14 caracteres, compuestas de 3 a 4 palabras aleatorias separadas por números y carácter especial más resistentes y memorizables.

2. **Restricciones de creación**

   Las credenciales no deben contener nombres de empresas, empleados o familiares, fechas, términos como runt, biometría o tránsito, ni secuencias como 123456 o qwerty.

Vigencia y rotación

No se exige rotación periódica obligatoria cada 30 o 90 días por inducir anotaciones inseguras se tora ante la alerta del T-Pot sobre fuerza bruta persistente o ante retiro de personal o sospecha de exposición (Grassi et al, 2017).

Gestión y custodia de credenciales

Se prohíbe la anotación en papel bajo el teclado o a vista de alumnos por restricción presupuestal se adopta KeePassXC local cifrado en equipos administrativos.

Implementación técnica inmediata

En Windows 10/11 Pro: secpol.msc directivas de cuenta, directiva de contraseñas longitud mínimo 14 caracteres bloqueo tras cinco intentos fallidos 15 minutos para frenar fuerza bruta.

Guía de configuración técnica de T-Pot

Requisitos mínimos de hardware

- Intel core i5/i7 o equivalente, mínimo 4 núcleos
- 16 gb ram requerida por elasricsearch/Kibana (Deutsche Telekom Security, 2024)
- SSd 128 gb por alta tasa de escritura de logs
- 1 tarjeta ethernet conectada al router Sagemcom

Preparación e instalación del T-Pot

Descargar e instalar debian 12 desde sitio oficial sin entorno grafico solo SSH server y standard system utilities. Actualización posterior

```
Sudo apt update && sudo apt upgrade –y
```

Descarga e instalación del T-Pot

Instalar curl: $ sudo [apt, dnf, zypper] install curlsi aún no está instalado

Clona el repositorio de GitHub: $ git clone https://github.com/telekom-security/tpotce

Cambie a la carpeta tpotce/:$ cd tpotce

Ejecute el instalador como usuario no root: $ ./install.sh

Durante el asistente de instalación se tiene que crear un usuario web administrativo con clave según política la política anterior y se tiene que reiniciar para la reasignación de puertos.

Reasignación de puerto

El instalador traslada el SSH de administrador del puerto 22 al 64295 y deja el puerto 22 expuesto como señuelo Cowrie todo intento con el puerto 22 cae en el contenedor.

Acceso al panel de control

Tablero Kibana: https://[IP_DEL_SERVIDOR_T-POT]:64297 consola cockpit https://[IP_DEL_SERVIDOR_T-POT]64294 el navegador mostrara advertencia por certificado auto firmado local se continúa ingresando el usuario y la contraseña.

Conclusión

Se cumplió el objetivo de proponer un esquema de endurecimiento de bajo costo para Aprendamos Ltda el análisis evidencio que la parte critica no estaba en la falta de equipos sino en compartir el router domestico Sagemcom, la red administrativa y Wi_Fi sin segmentación y con las credenciales por defecto.

El despliegue de la plataforma T-Pot con sus herramientas permitió contar con las alertas tempranas donde antes no había visibilidad, desvió de escaneos y fuerza bruta a señuelos sin afectar la operación principal gracias al IRP basado en NIST SP 800-61 nos ayudo a cerrar las brechas de los datos mas vulnerables como las contraseñas hallas con los recursos utilizados.

Referencias

Centro de Enseñanza Automovilística Aprendamos Ltda. Proyecto Educativo Institucional

Cichonski, P, Millar, T Grancé, T & Scarfone, K (2012). Computer security incident Handling guide: Recommendations of the national institute of standards and technology (SP 800-61 Rev. 2) national institute of standards and technology https://doi.org/10.6028/NIST.SP.800.61r2

congreso de Colombia (2012) ley 1581 de 2012 por la cual se dicta disposiciones generales para la protección de datos personales. Diario oficial.

Crowdstrike. (2024) ¿Qué es un honeypot en ciberseguridad? https://www.crowdstrike.com/es-es/cybersecurity-101/exposure-management/honeypots/

Deutsche Telekom Security (2024). T-Pot – the all in one multi honeypot platform [repositorio] GitHub https://github.com/telekom-security/tpotce

Dionaea Project (2023) dionaea documentación https://github.com/DinoTools/dionaea

Elastic (2024a) Elasticsearch guide. https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html

Elastic (2024b) Kibana guide https://wwwelastic.co/guide/en/kibana/current/index.html

EMIS (2026) perfil compañía centro de enseñanza automovilística aprendamos Ltda. https://www.emis.com/

Grassi P.A, Garcia M.E & Fenton J.L, (2017) digital identity guidelines authentication and lifecycle management (SP 800-63B) national institute of standards and technology https://pages.nist.gov/800-63-3/sp800-63b.html

INCIBE-CERT (2023) honeypot, una herramienta para conocer al enemigo https://www.incibe.es/incibe-cert/blog/honeypot-herramienta-conocer-al-enemigo

international organization for standardization (2015) ISO 9001:2015 Quality management systems – Requirements. ISO

MITRE (2024) MITRE ATT&CK framework https://attack.mitre.org/

Oosterhoff, M (2024) Cowrie SSH/Telnet honeypot [Repositorio] GitHub https://github.com/cowrie/cowrie

Rist, L et al (2024) Conpot – ICS/SCADA honeypot. https://github.com/mushorg/compot

Spitzner, L (2003) MITRE ATT&CK: Design and philosophy. MITRE

Wemer, T (2003) Honeypot documentation https://github.com/honeytrap/honeytrap