ERIC GROSSERMANN

01.09.2026

4GEEKS ACADEMY

CYBERSECURITY PROYECTO FINAL

#latam-pt-cs-8

PROCESO DE LA INVESTIGACION

Este proyecto tiene como propósito analizar un incidente de seguridad, corregir las debilidades identificadas y fortalecer la protección de un servidor crítico comprometido dentro de un entorno simulado, asumiendo el rol de analista de ciberseguridad.

Para lograrlo, el trabajo se organizó en tres fases principales, cada una orientada a abordar el problema desde una perspectiva distinta y complementaria.

FASE 1 – ANÁLISIS FORENSE Y CONTENCIÓN

Identificación del vector de ataque, recolección de evidencias, contención y corrección del incidente para evitar la escalación del ataque.

FASE 2 – DETECCIÓN Y CORRECCIÓN DE VULNERABILIDADES

Búsqueda de nuevas vulnerabilidades distintas al ataque original, explotación dentro de un entorno controlado.

FASE 3 – RESPUESTA A INCIDENTES Y SGSI

Diseño de un plan de respuesta basado en NIST y desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con la norma ISO/IEC 27001 para prevenir futuros incidentes

POR QUE?

¿POR QUÉ SE DIVIDIÓ EL PROYECTO EN TRES FASES?

El proyecto se dividió en tres fases distintas para reducir riesgos de forma progresiva, evitar pérdidas económicas innecesarias y asegurar la continuidad operativa del servidor crítico de la Academia.
Cada fase cumple un objetivo específico dentro del negocio y evita costos y perdidas economica distintas

Fase 1 – Contención

El objetivo fue detener el daño inmediato y recuperar el control del sistema.Si el acceso no autorizado continuaba activo, la Academia podía enfrentar:

- Pérdida de información
- Interrupción de servicios
- Costos elevados por incidentes no controlados

Fase 2 – Reducción de Riesgo

Una vez controlado el incidente, el enfoque fue reducir la superficie de ataque.
Se corrigieron vulnerabilidades adicionales que, de no atenderse, podían generar:

- Nuevos incidentes
- Afectación a la reputación de la Academia

Cada fase reduce el riesgo y aumenta el nivel de control y madurez de seguridad.

Fase 3 – Prevención

Con El objetivo final de evitar que el incidente vuelva a ocurrir.
Se diseñaron controles y un enfoque alineado con NIST e ISO para:

- Mejorar la detección temprana
- Reducir tiempos de respuesta

Esta fase transforma un incidente en una inversión en seguridad, reduciendo costos a largo plazo y fortaleciendo la madurez de la organización.

FASE 1 – RECONOCIMIENTO Y RECOLECCIÓN DE EVIDENCIAS

OBJETIVO: ENTENDER COMO EL ATACANTE COMPROMETIO EL SERVIDOR? EVITAR LA CONTINUACION Y LA ESCALADA DEL ATAQUE.

LAS ACTIVIDADES PRINCIPALES DE ESTA FASE SE CENTRARON EN:

Evaluacion de los Procesos del Sistema

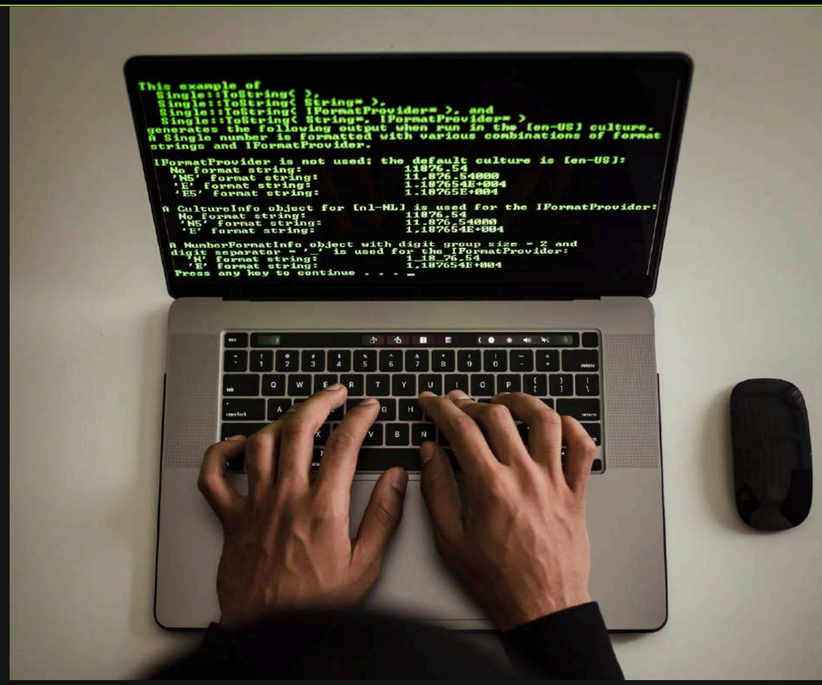
El objetivo de identificar archivos sospechosos, procesos en ejecución anómalos o cualquier modificación inusual

Revisión de registros del sistema

Especialmente logs de autenticación para detectar accesos no autorizados y comportamientos anómalos.

Escaneo del sistema

para descartar la presencia de rootkits o malware persistente usando herramientas como chkrootkit y rkhunter.



El resultado de esta fase permitió obtener una visión clara del incidente, sentando las bases para la contención, corrección de vulnerabilidades y fortalecimiento posterior del sistema.

ANALISIS DE LOS RESULTADOS

Este procedimiento permitió reconstruir el evento de seguridad, confirmar el vector de ataque y definir las acciones necesarias para la contención y corrección del incidente.

Registro de ataque:
08 de octubre a las
17:40pm

Ip del ataque:
192.168.0.134

Servicio Expuesto:
SSH

Resolucion:

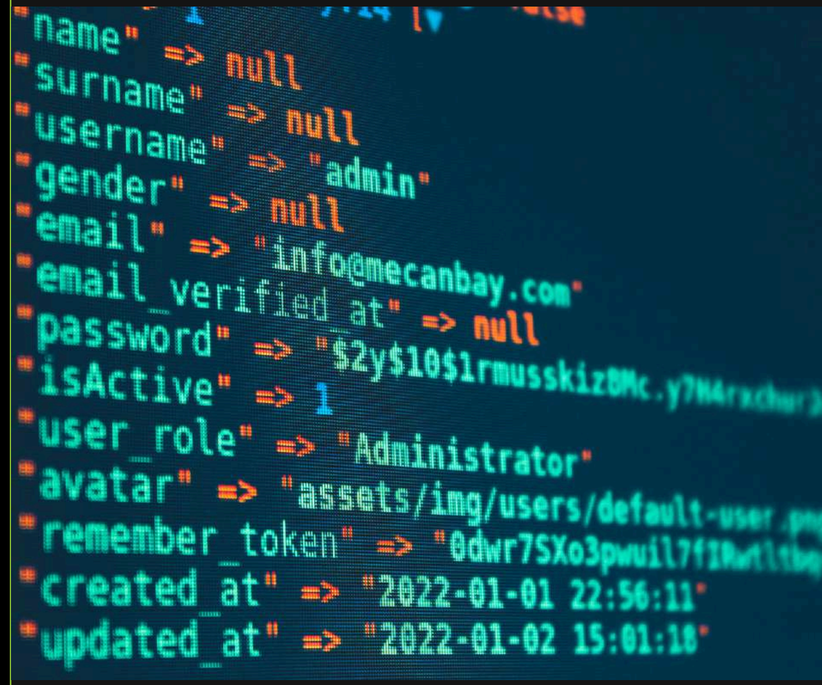
- **Implementacion Firewall**
- **Actualizacion del Kernel**
- **Detencion de servicios Ftp y Apache**

FASE 2: DETECCIÓN Y CORRECCIÓN DE UNA NUEVA VULNERABILIDAD

ESTA FASE BUSCA DEMOSTRAR QUE UN SISTEMA COMPROMETIDO PUEDE PRESENTAR MÚLTIPLES DEBILIDADES, INCLUSO DESPUÉS DE CORREGIR EL PRIMER ATAQUE, Y QUE ES NECESARIO REALIZAR UNA EVALUACIÓN PROACTIVA PARA REDUCIR LA SUPERFICIE DE ATAQUE.

COMO SE REALIZO?

SE UTILIZARON HERRAMIENTAS COMO NMAP, PARA UNA RECOPILACION ADICIONAL DE INFORMACION DE NUEVAS VULNERAVILIDADES.



SOLUCION

ENUMERACION DE VULNERAVILIDADES

Vulnerabilidad	Descripción	Nivel de Criticidad
Acceso administrativo sin autenticación	El usuario "root" permite acceso al motor de base de datos sin requerir contraseña.	CRÍTICO
Exposición de bases de datos sensibles	Se logró enumerar bases de datos internas, incluyendo una base de datos activa de **WordPress**.	CRÍTICO
Superficie de ataque por servicio crítico activo	El servicio de base de datos está activo y accesible localmente.	ALTO

IMPACTO EJECUTIVO DEL INCIDENTE

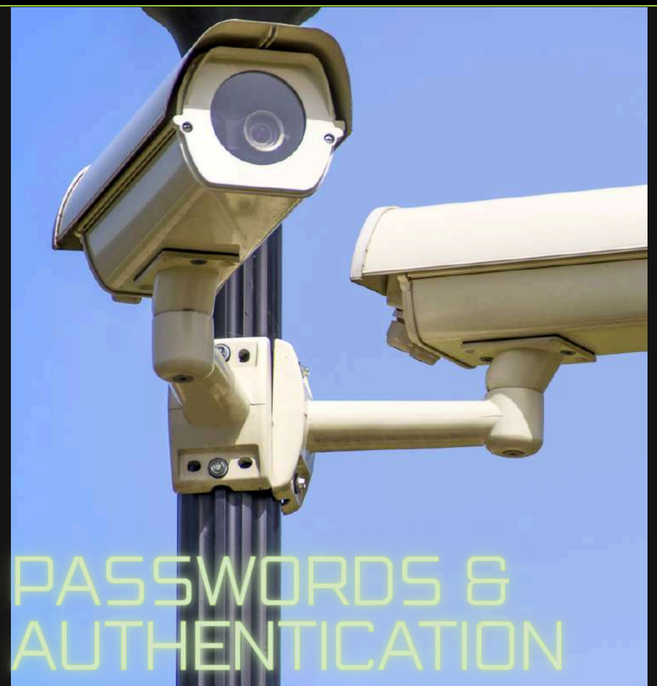
FASE 3: PLAN DE RESPUESTA A INCIDENTES

¿Por qué esta fase es clave?

Porque detectar y corregir no es suficiente si la organización no sabe cómo actuar ante un nuevo incidente.

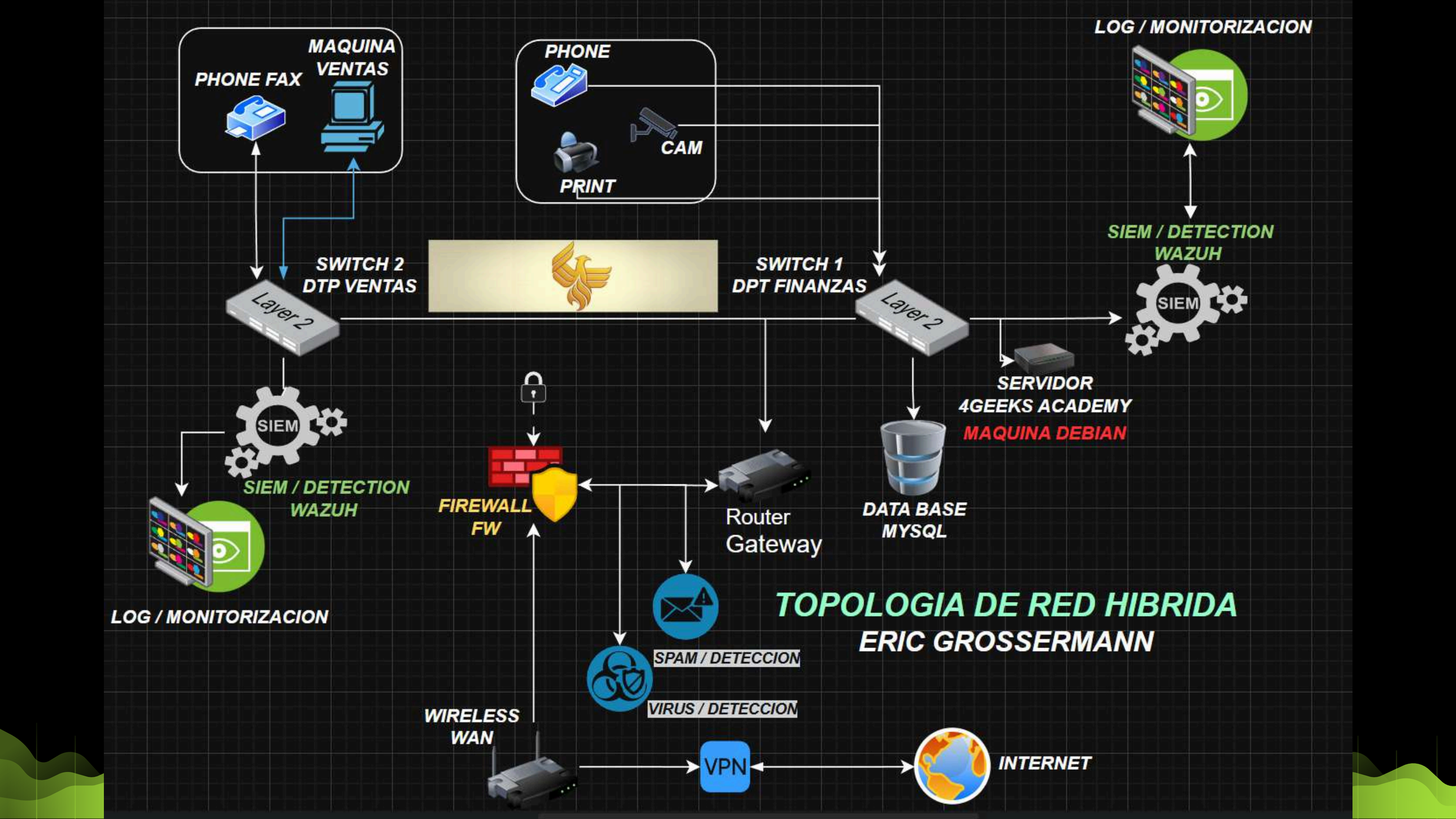
🔐 Endurecimiento de Accesos SSH
🌐 Reducción de Superficie de Ataque
🚫 Mitigación Automática de Ataques
📊 Monitoreo y Detección (SIEM – Wazuh)
👤 Gestión de Credenciales y Privilegios
🏛️ Alineación con Estándares de la Industria

Controles Implementados



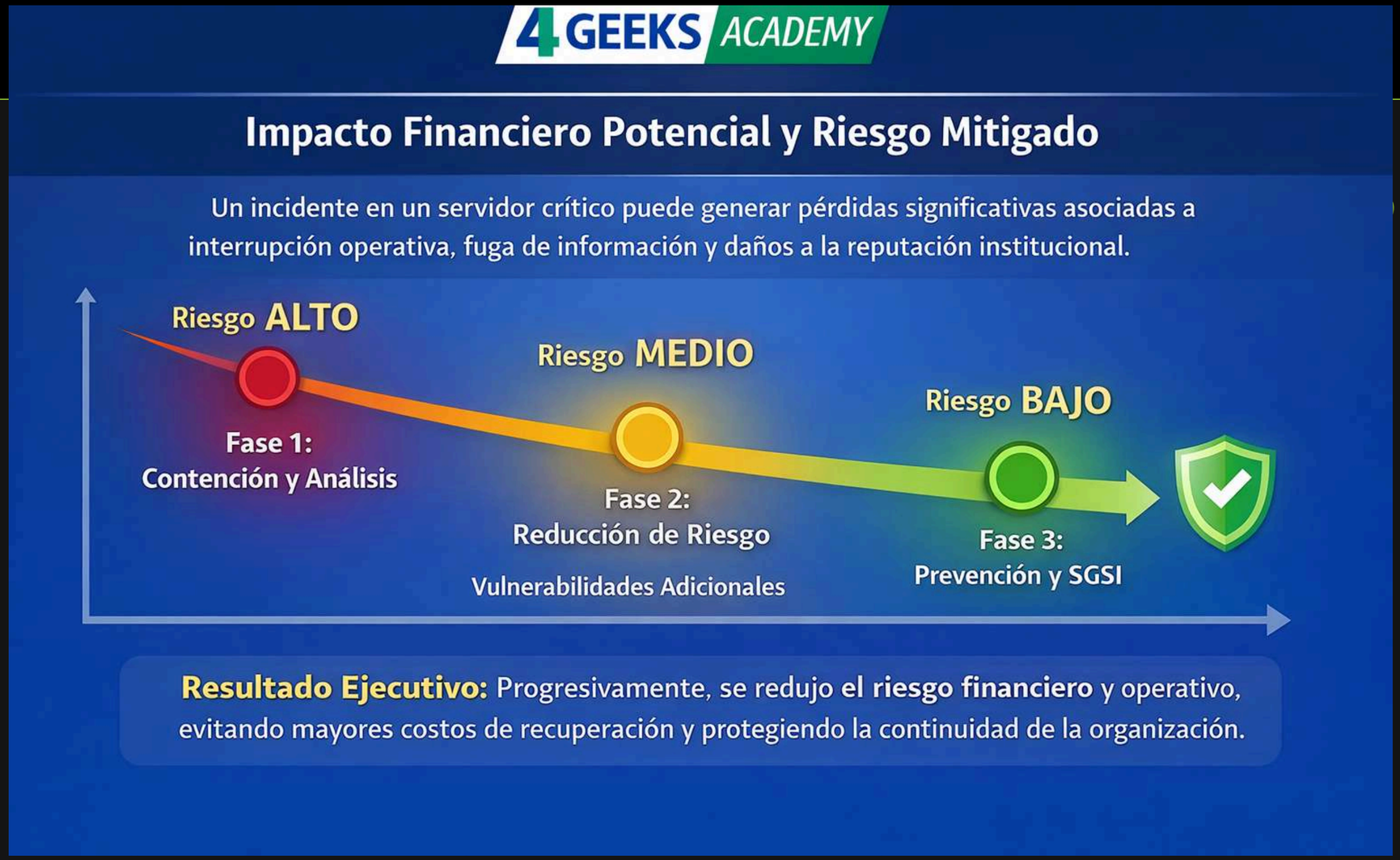
Impacto para la organización

- Reducción del tiempo de respuesta
- Menor riesgo de interrupción operativa
- Disminución de costos por incidentes repetidos
- Mayor madurez y resiliencia en seguridad


MAQUINA VENTAS
PHONE FAX
PHONE
CAM
PRINT
LOG / MONITORIZACION
SIEM / DETECTION WAZUH
SWITCH 2 DTP VENTAS
SWITCH 1 DPT FINANZAS
Layer 2
Layer 2
SIEM
SIEM
SERVIDOR 4GEEKS ACADEMY MAQUINA DEBIAN
SIEM / DETECTION WAZUH
FIREWALL FW
Router Gateway
DATA BASE MYSQL
LOG / MONITORIZACION
TOPOLOGIA DE RED HIBRIDA
ERIC GROSSERMANN
SPAM / DETECCION
VIRUS / DETECCION
WIRELESS WAN
VPN
INTERNET

IMPACTO FINANCIERO ESTIMADO Y RIESGO MITIGADO

Un acceso no autorizado a un servidor crítico puede generar pérdidas significativas asociadas a interrupción operativa, fuga de información, recuperación técnica y reputación institucional.



Mediante esta investigacion queda comprobado que, la seguridad ya no es un costo operativo, sino una decisión estratégica que protege los activos, la continuidad y el valor del negocio.