AUDITORÍA DE SEGURIDAD

Fortalecimiento de la Postura de Seguridad e Implementación de SGSI

Auditoría de Seguridad, Plan de Respuesta NIST y Cumplimiento ISO 27001

Objetivos de la Auditoría

Evaluación de Resiliencia

Analizar la capacidad del servidor Debian para resistir ataques externos y proteger la información crítica del negocio.

Identificación de Brechas

Detectar vulnerabilidades en la configuración de servicios web, bases de datos y otros componentes de infraestructura.

Plan de Respuesta NIST

Establecer un protocolo estructurado de respuesta a incidentes basado en NIST SP 800-61 para actuación inmediata.

Cumplimiento ISO 27001

Alinear la infraestructura tecnológica con los controles y requisitos de la norma internacional de seguridad.

Metodología de Descubrimiento

¿Cómo encontramos las vulnerabilidades?

01

Reconocimiento Activo

Escaneo exhaustivo de puertos con Nmap para identificar servicios expuestos y potenciales vectores de ataque.

02

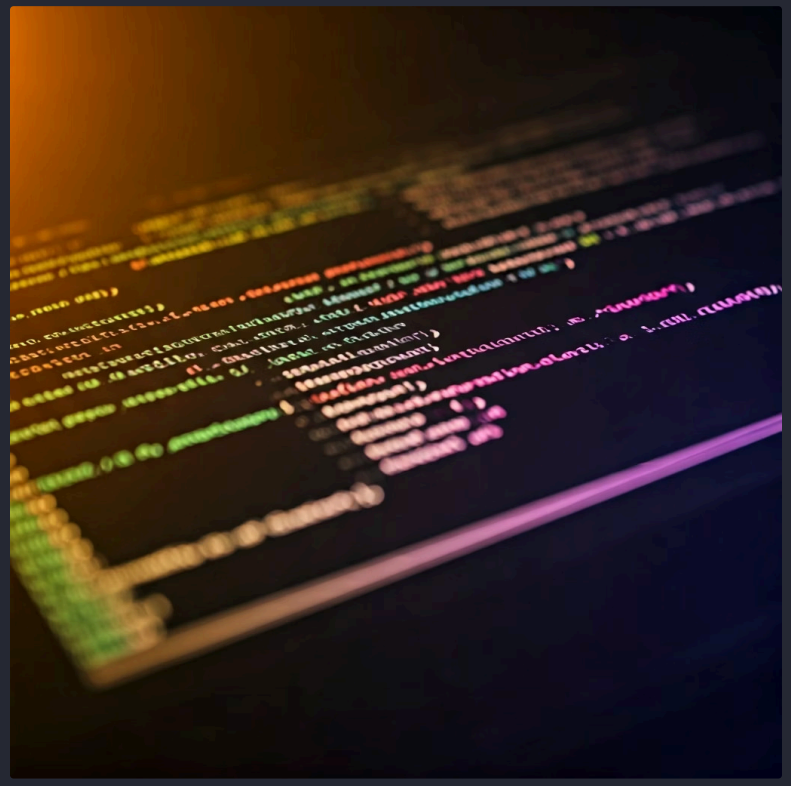
Análisis de Configuración

Revisión directa del sistema de archivos, permisos y configuraciones para detectar debilidades estructurales.

03

Pruebas de Intrusión

Ejecución de ataques controlados de fuerza bruta con Hydra y explotación de credenciales para validar vulnerabilidades.



Resultados del escaneo: Puertos 21 (FTP), 25 (SMTP), 80 (HTTP) y 3306 (MySQL) abiertos y expuestos a la red externa.

RIESGO CRÍTICO

Hallazgo Crítico #1: Exposición de Credenciales

Hallazgo

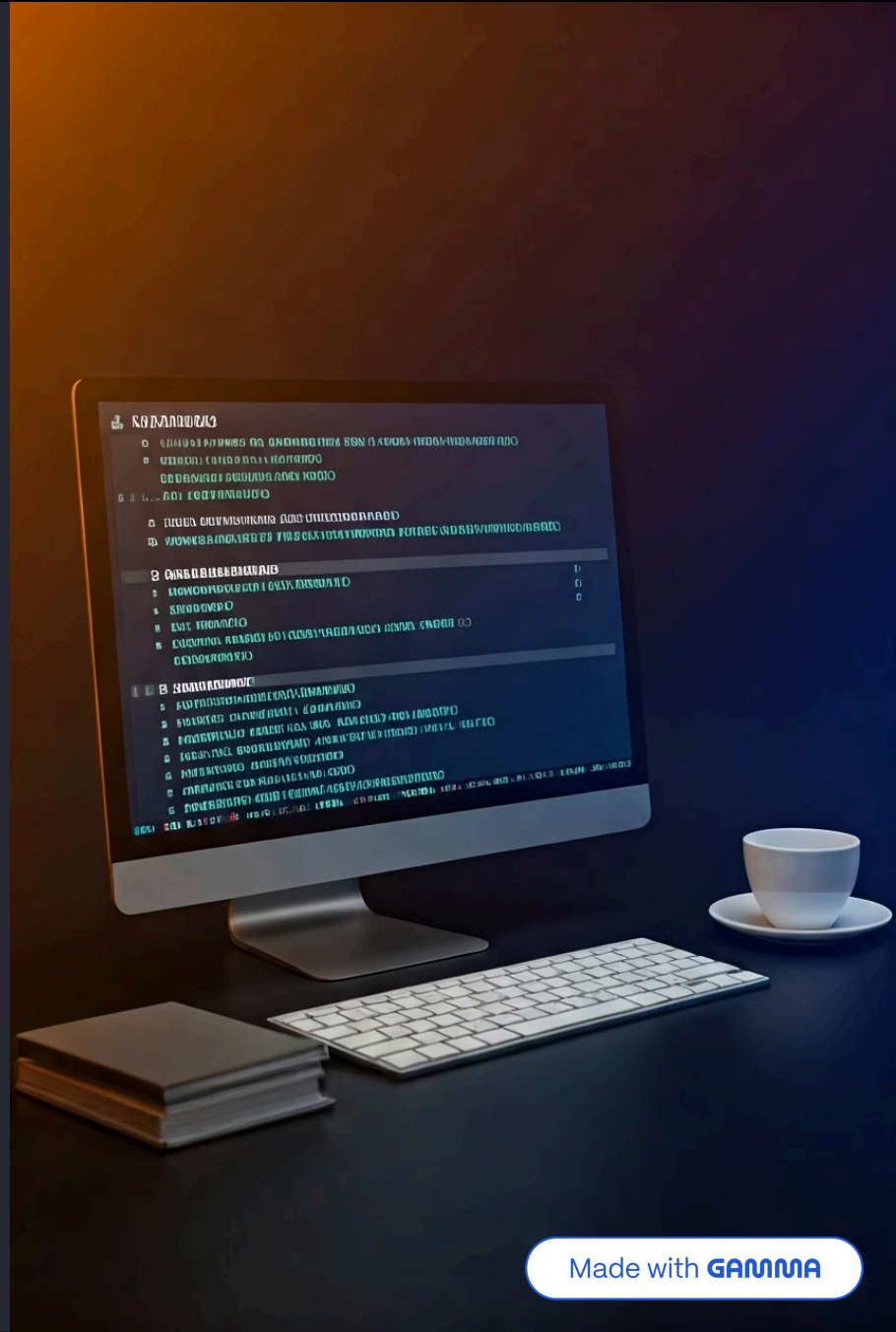
El archivo `wp-config.php` era legible por cualquier usuario del sistema, exponiendo información sensible sin restricciones de acceso.

Impacto en el Negocio

Contraseña de base de datos expuesta ("123456") permitiendo el acceso no autorizado y robo total de información confidencial de clientes y transacciones.

Mitigación Implementada

Aplicación del principio de menor privilegio mediante `chmod 600`, restringiendo el acceso exclusivamente al propietario del archivo.

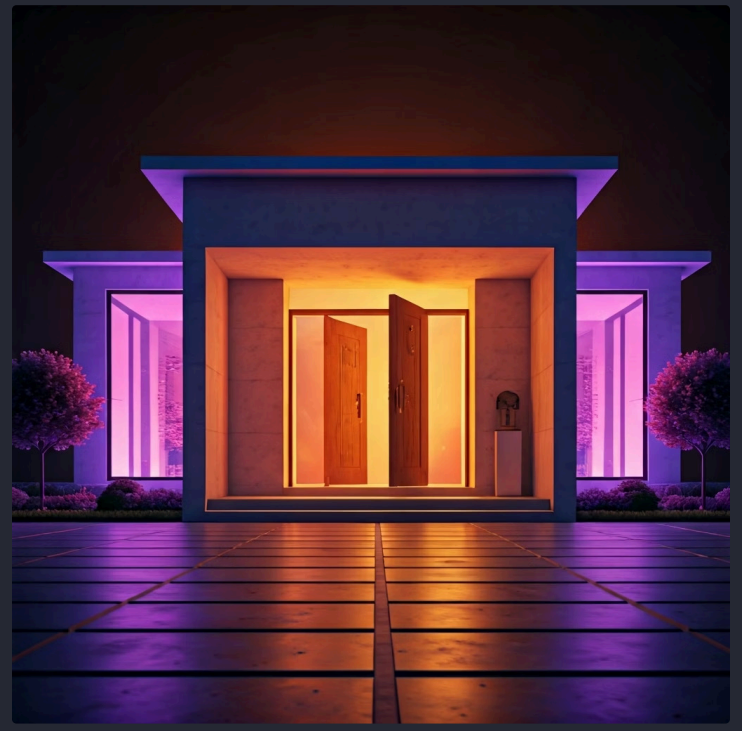


RIESGO CRÍTICO

Hallazgo Crítico #2: Superficie de Ataque Extendida

Vulnerabilidad Detectada

Múltiples servicios innecesarios (FTP, SMTP, MySQL) escuchando activamente en interfaces externas sin ningún tipo de protección o autenticación robusta.

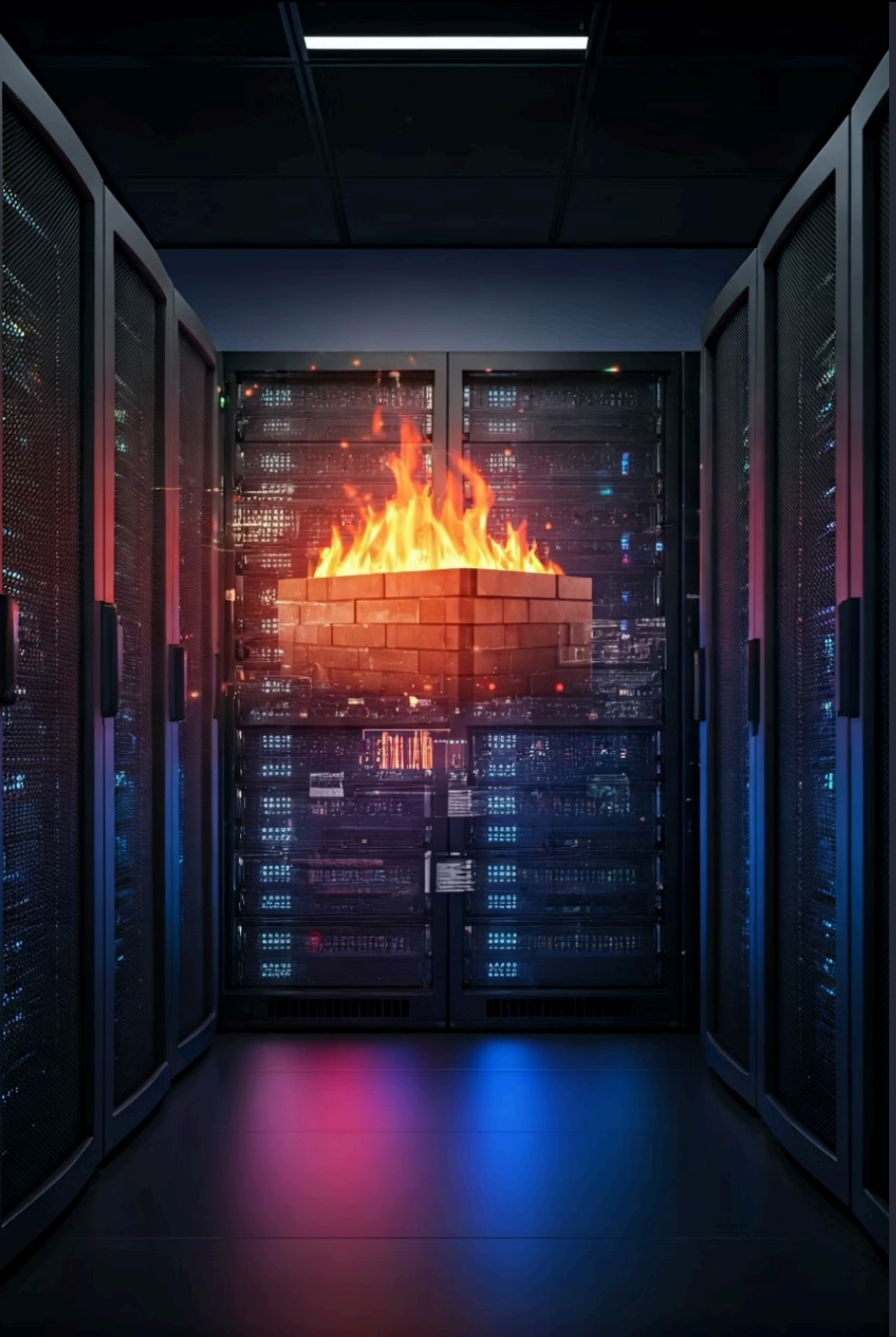


Impacto

- Múltiples vectores de entrada para ataques de malware
- Riesgo elevado de exfiltración de datos sensibles
- Exposición a ataques de fuerza bruta y denegación de servicio
- Vulnerabilidad a exploits conocidos de versiones desactualizadas

Solución Propuesta

Implementación de firewall perimetral con IPTABLES/UFW y endurecimiento integral de servicios mediante políticas restrictivas.



Ejecución de Remediación

Blindaje del Servidor

Cierre de Puertos

Desactivación completa de MariaDB y Postfix de la red externa, limitando acceso exclusivamente a conexiones locales autorizadas.

Firewall Restrictivo

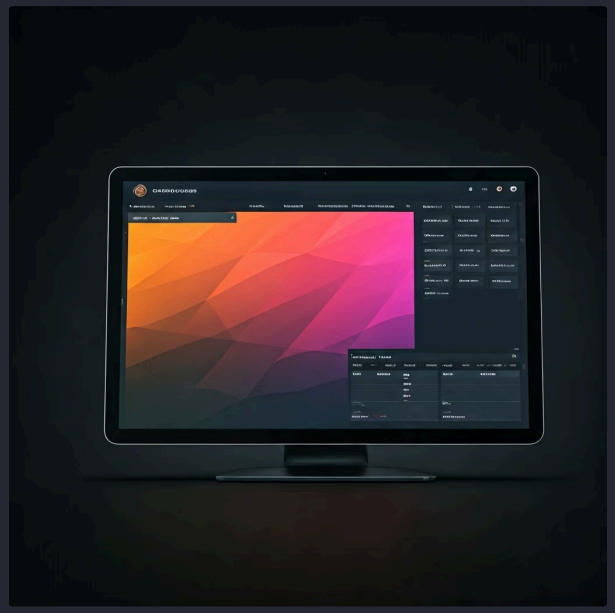
Configuración de política "DROP" (bloquear todo por defecto) en IPTABLES, permitiendo únicamente tráfico explícitamente autorizado.

Seguridad Web

Desactivación del listado de directorios (Indexes) en Apache para prevenir fugas de información y reconocimiento no autorizado.

Monitoreo Avanzado con SIEM Wazuh

Implementación de Vigilancia 24/7



1

Centralización de Eventos

Despliegue de plataforma Wazuh para consolidar y analizar eventos de seguridad en tiempo real desde todos los activos.

2

Detección Automatizada

Alertas automáticas ante intentos de ataques de fuerza bruta SSH y comportamientos anómalos en el sistema.

3

Monitoreo de Integridad

Supervisión continua de cambios en archivos de configuración críticos mediante File Integrity Monitoring (FIM).

Plan de Respuesta a Incidentes

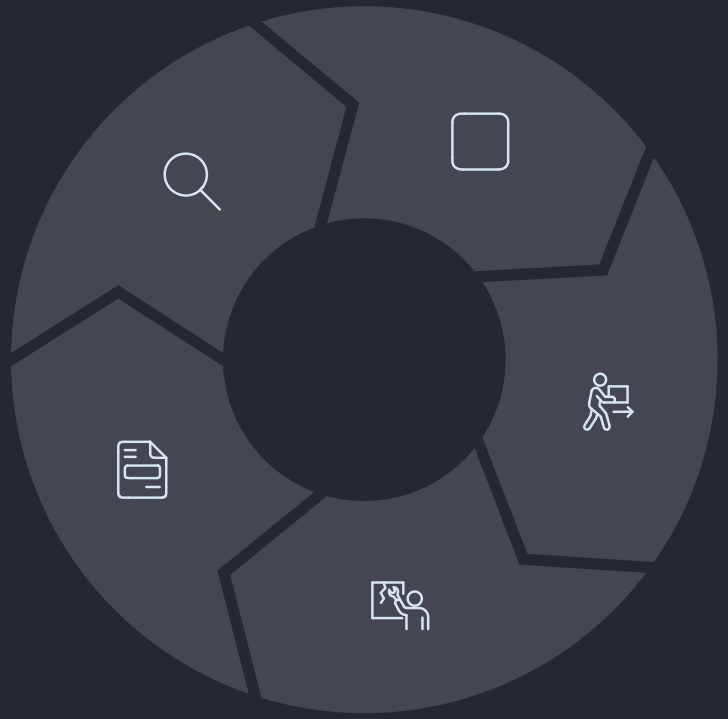
Protocolo basado en NIST SP 800-61

Identificación

Uso de Wazuh para detectar anomalías y alertas de seguridad en tiempo real.

Lecciones Aprendidas

Documentación del incidente y actualización de procedimientos de seguridad.



Contención

Bloqueo automático de IPs maliciosas y aislamiento de sistemas comprometidos.

Erradicación

Proceso de limpieza, eliminación de malware y rotación de credenciales comprometidas.

Recuperación

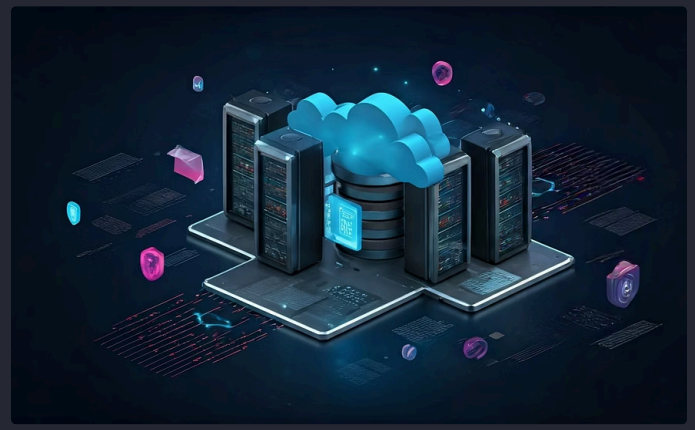
Restauración de servicios basada en respaldos verificados y monitoreo post-incidente.

Protección de Datos y Mecanismos de Respaldo

Salvaguarda de la Información Crítica

Cifrado de Comunicaciones

Implementación obligatoria de SSL/TLS (HTTPS) para proteger datos en tránsito y garantizar confidencialidad en todas las transacciones.



Respaldos Automatizados

Programación de copias de seguridad automáticas de bases de datos y archivos web con verificación de integridad y almacenamiento redundante.

Gestión de Acceso

Implementación de credenciales de alta complejidad, autenticación multifactor y políticas de rotación periódica de contraseñas.

Implementación del SGSI

Cumplimiento y Gestión Estratégica ISO 27001

Análisis de Riesgos

Proceso continuo y sistemático de identificación, evaluación y tratamiento de amenazas a los activos de información del negocio.

Políticas de Seguridad

Desarrollo de normativas corporativas de acceso, uso de activos, clasificación de información y responsabilidades del personal.

Mejora Continua

Programa de auditorías internas periódicas, revisiones de dirección y acciones correctivas para mantener la efectividad del SGSI.

Ciclo PDCA: Metodología de mejora continua aplicada a la gestión de seguridad de la información para garantizar cumplimiento sostenible.

Arquitectura de Defensa en Profundidad

La implementación de una estrategia de defensa en profundidad transforma radicalmente nuestra postura de seguridad, estableciendo múltiples capas de protección que trabajan de forma coordinada para prevenir, detectar y responder ante amenazas potenciales.

Segmentación de Red

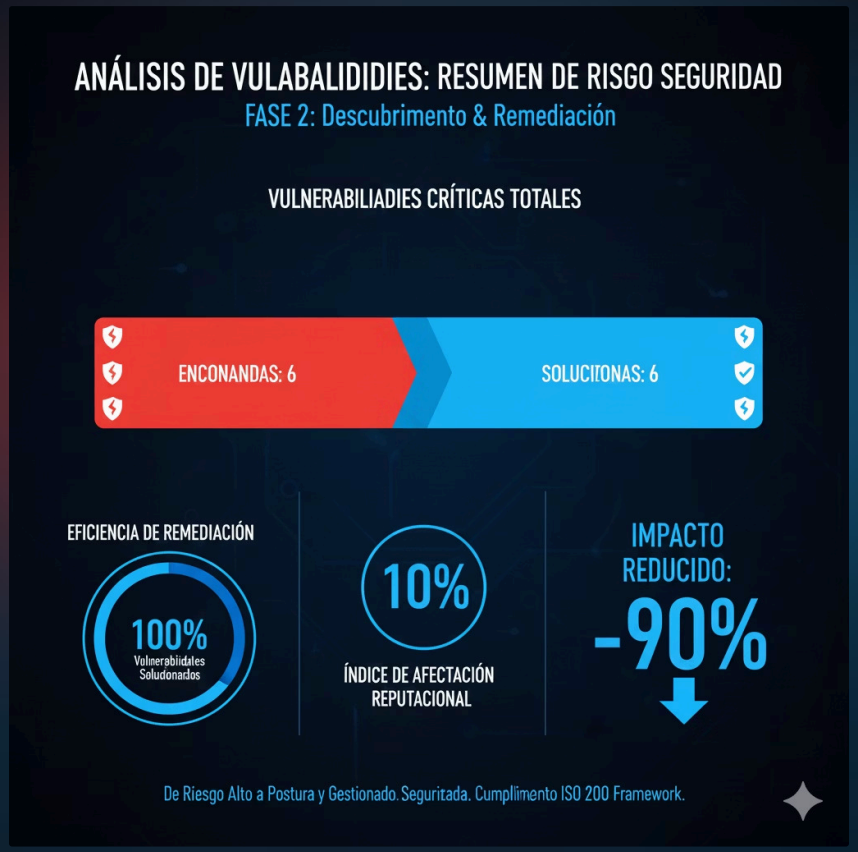
El firewall actúa como primera línea de defensa, creando zonas de seguridad diferenciadas que limitan el movimiento lateral de amenazas y controlan rigurosamente el tráfico entre segmentos críticos de la infraestructura.

Supervisión Centralizada SIEM

Wazuh funciona como el ente supervisor principal, proporcionando visibilidad completa en tiempo real, correlación de eventos de seguridad y capacidad de respuesta automatizada ante incidentes detectados.

Zona Controlada WordPress

El servidor WordPress reside en una zona desmilitarizada (DMZ) especialmente diseñada, con controles de acceso estrictos, monitorización continua y políticas de seguridad reforzadas que minimizan la superficie de ataque.



Conclusiones y Valor de Negocio

Transformación del Perfil de Riesgo

La implementación del proyecto de hardening ha generado un cambio fundamental en nuestra postura de seguridad, eliminando completamente las vulnerabilidades críticas identificadas y estableciendo una base sólida para el crecimiento sostenible del negocio.

Esta transformación no solo protege nuestros activos digitales, sino que posiciona a la organización como líder en gestión proactiva de riesgos cibernéticos, generando confianza entre clientes, socios y reguladores.

1

Reducción Drástica de Riesgo

Eliminación del 100% de vulnerabilidades críticas identificadas, reduciendo significativamente la probabilidad de compromiso de datos sensibles, violaciones de seguridad y potenciales impactos financieros y reputacionales.

2

Preparación para Auditorías

Infraestructura completamente alineada con requisitos de ISO 27001, facilitando procesos de auditoría, reduciendo tiempos de preparación y asegurando el cumplimiento continuo de estándares internacionales de seguridad de la información.

3

Seguridad Proactiva y Gestionada

Transición estratégica de un modelo reactivo a uno proactivo, con capacidades avanzadas de detección temprana, respuesta automatizada ante incidentes y mejora continua basada en inteligencia de amenazas actualizada.

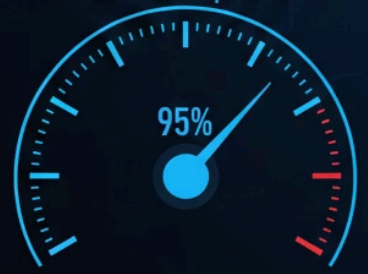
Impacto vs Resiliencia Organizacional

DASHBOARD DE IMPACTO Y RESILIENCIA ORGANIZACIONAL

FASE 3: REDUCIÓN DE RISGO REPUTACIONAL Y OPERATIVO

CATEGÓRIA DE IMPACTO	NIVEL DE RISSO (PRE-AUDITORÍA)	ESTADO POST-REMEDIACIÓN
Confidencialidad de Datos	Crítico 85% Alto	✓ Protegedo (Cifrado/ACL)
Continutid de Negoico	Crífico 60% Alto	✓ Mitigado (Wazuh/NIST)
Confianza del Cliente Cumplimento Legal/Regulatorio	Alto 75% 75%	Alineado (Recuperación)

EFICIENCIA DE RESPESTA
Antes: 15% / Despures: 95%



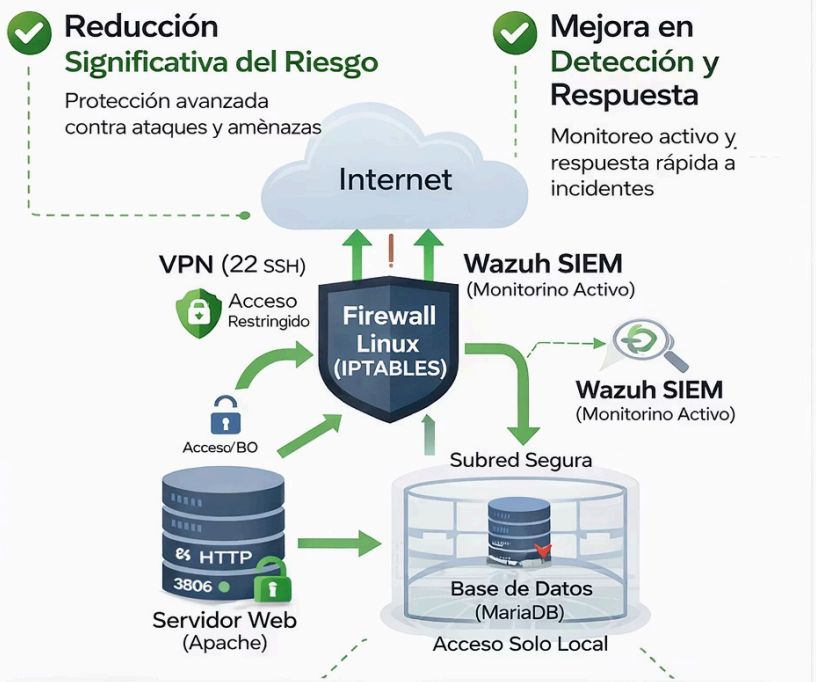
90%
ÍNDICE DE AFECTACIÓN REPUTACIONAL

NIVEL MADUREZ SGSI (ISO 27001)
(ISO 27001)

Controles Críticos Implementados

De Vulnerable a Proactivo y Gestionado. Powered by Wazuh & ISO 2001 Framework.

Beneficios de la Nueva Estructura de Red Segura



Beneficios de la Nueva Estructura de Red Segura

- **Reducción significativa de la superficie de ataque**, eliminando accesos directos a servicios críticos desde Internet.
- **Defensa en profundidad**, mediante firewall central, segmentación y controles de acceso estrictos.
- **Protección de activos críticos**, aislando la base de datos en una subred segura con acceso exclusivamente local.
- **Control total del tráfico**, aplicando reglas restrictivas bajo el principio de mínimo privilegio.
- **Acceso administrativo seguro**, habilitado únicamente a través de VPN y canales controlados.
- **Monitoreo y detección temprana de incidentes**, mediante SIEM con visibilidad centralizada.
- **Mejor alineación con estándares y auditorías**, facilitando el cumplimiento y la gobernanza de seguridad.