INFORME OFICIAL DE INCIDENTE DE SEGURIDAD

ATAQUE DDoS AL SERVIDOR APACHE

Fecha del incidente: 18 al 22 de septiembre de 2025

Área responsable: Tecnologías de la Información y Comunicaciones (TIC's)

Sistema afectado: Servidor Apache – Infraestructura de proyectos QR y SCP

1. RESUMEN EJECUTIVO

El 18 de septiembre de 2025 se detectó un ataque de denegación de servicio distribuido (DDoS) dirigido al servidor Apache, el cual generó un volumen inusual de peticiones HTTP simultáneas provenientes de múltiples direcciones IP. El evento causó una saturación temporal del servicio web, sin comprometer la integridad de la información ni afectar las bases de datos productivas. El incidente fue controlado y mitigado el 22 de septiembre de 2025 a las 16:00 horas, restableciendo los servicios de manera segura.

2. ANÁLISIS DEL INCIDENTE

Durante el ataque se registraron numerosos intentos de acceso no autorizado, los cuales fueron bloqueados mediante reglas de firewall y filtrado de IPs. El análisis forense posterior reveló que el archivo `.env` fue expuesto temporalmente, lo que implicó la posibilidad de acceso a credenciales y datos sensibles del sistema, incluyendo conexiones a la base de datos principal. Se actuó de manera inmediata para revocar los accesos comprometidos, restringir permisos, reconfigurar la seguridad del servidor y fortalecer las políticas de resguardo de credenciales. A pesar de esta exposición, no se detectaron accesos indebidos ni alteraciones en los registros o estructuras de la base de datos. La integridad y confidencialidad de la información permanecieron intactas.

3. MEDIDAS DE CONTENCIÓN INMEDIATAS

Durante el proceso de mitigación se llevaron a cabo las siguientes acciones:

- Eliminación de archivos potencialmente vulnerables.
- Reconfiguración de rutas de acceso internas.
- Revisión y restricción de acceso al archivo `.env`, limitándolo exclusivamente al usuario webmaster.
- Refuerzo de permisos de seguridad y cifrado del archivo `.env`, garantizando su protección ante futuras fugas de información.
- Reinicio y endurecimiento de la configuración del servicio Apache.
- Suspensión temporal de servicios Python y de envío de correos electrónicos.

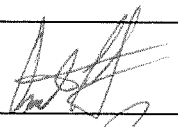
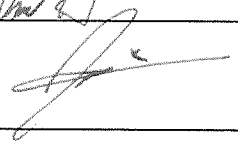
8. RECOMENDACIONES Y ACCIONES:

- Mantener monitoreo constante durante las próximas 72 horas posteriores al evento.
- Ejecutar verificaciones semanales de permisos y logs del servidor.
- Implementar auditorías mensuales de seguridad.
- Realizar, en coordinación con los proveedores R&J y SkyMeduza, el cambio de contraseñas de:

  - VPN corporativa.
  - Accesos al sistema SCP.
  - Plataformas relacionadas.
  - Base de datos principal.

Este procedimiento se programará en el periodo de menor flujo operativo (diciembre-enero) para evitar afectaciones al servicio.

8. RESPONSABLES DE CONTINUIDAD DE SERVICIO E INFORME

Nombre	Cargo	Firma
Ing. Oswaldo Daniel Ortiz Martinez	Jefe de TIC's	
Ing. Emanuel Simón Zepeda	Desarrollador Analista	
Ing. Jaime Armando Comparan Velasco	Desarrollador WEB	