ESTADO DE CIBERSEGURIDAD Y RECUPERACIÓN

- Informe Ejecutivo
- Análisis y respuesta ante incidentes de seguridad informática.
- Abril 2025

RESUMEN EJECUTIVO

- Se ha llevado a cabo un análisis completo tras la detección de un incidente de seguridad.
- El informe cubre la identificación de vulnerabilidades críticas, su explotación, y las acciones correctivas aplicadas.
- Además, se ha implementado un plan de recuperación y continuidad operativa.

RESPUESTA ANTE EL INCIDENTE

- • Monitoreo de logs del sistema para identificar accesos maliciosos.
- • Escaneo con herramientas de detección de malware (rkhunter).
- • Aislamiento y limpieza de configuraciones comprometidas.
- • Revisión completa de servicios y archivos clave del sistema.

VULNERABILIDADES DETECTADAS

- 1. Acceso SSH con root habilitado: permitía accesos directos sin restricciones.
- 2. Servicio FTP inseguro: permitía conexiones anónimas sin cifrado.
- 3. Apache configurado para mostrar archivos de directorios (Indexing).
- 4. Permisos inseguros en wp-config.php: exposición de credenciales sensibles.

ACCIONES CORRECTIVAS

- • Deshabilitado el acceso root por SSH (PermitRootLogin no).
- • Reconfigurado o desactivado el servicio FTP para prevenir accesos anónimos.
- • Cambiados los permisos de wp-config.php para proteger información crítica.
- • Desactivada la opción Indexes en Apache para evitar exposición de archivos.
- • Aplicadas reglas de firewall que restringen el tráfico HTTP no autorizado.

RECUPERACIÓN Y CONTINUIDAD

- • Se utilizaron respaldos externos para restaurar servicios críticos.
- • Se verificó la integridad de los datos restaurados.
- • Se estableció un plan de continuidad para minimizar el tiempo de inactividad.
- • Se alineó el proceso con las directrices de la norma ISO 27001.

RECOMENDACIONES EJECUTIVAS

- • Fortalecer las políticas de contraseñas y autenticación.
- • Monitoreo constante de logs de seguridad y servicios.
- • Realizar auditorías regulares del sistema.
- • Minimizar privilegios root y aplicar principio de menor privilegio.
- • Implementar un SGSI formal que contemple análisis de riesgos y continuidad.

CONCLUSIÓN

- El entorno ha sido asegurado tras identificar y corregir múltiples fallos de configuración.
- Se garantiza la continuidad operativa mediante respaldos y políticas de recuperación.
- Se han planteado acciones estratégicas para evitar incidentes similares en el futuro.
- La organización fortalece su postura de seguridad de forma proactiva.