Warriors®
SingularityRISK

La solución **Warriors Singularity Risk®** ofrece una serie de ventajas sobre cualquier otra plataforma, destacando la facilidad de uso, adaptación de procesos y prácticas que permiten la gestión y tratamiento de riesgos de su compañía, enfocados a las vulnerabilidades detectadas en los escaneos estáticos y dinámicos, pruebas de penetración y campañas de phishing, así como a la verificación del tratamiento de las riesgos y vulnerabilidades existentes.

La solución se puede desplegar en las instalaciones de su compañía en modalidad **On-Premise**, eliminando los riesgos de compartir las aplicaciones con terceras partes en la nube.

Estas son algunas de las características más importantes de esta versión:

- **La solución es escalable.**
- **Es adaptable a sus procesos, procedimientos y flujos operativos y personalización de campos de información necesarios.**
- **Funcionalidades adaptables a sus necesidades.**
- **Un despliegue rápido y preciso, acorde a sus lineamientos.**
- **La solución le ofrece un nuevo enfoque de gestión de riesgos acorde a las mejores prácticas internacionales, definiendo sus propios catálogos, niveles de riesgo y cálculos de probabilidad, impacto, frecuencias.**
- **Definir la clasificación de información de acuerdo con sus niveles de sensibilidad o disponibilidad, así como los responsables del tratamiento de los riesgos.**
- **Definir su catálogo de controles, acciones de remediación, responsables y fechas compromiso de solución.**
- **Definir y documentar planes de mitigación, de acción, seguimiento, responsables, estatus de actividades, alertamiento preventivo y de vencimiento.**
- **Administrar la evidencia digital de las acciones realizadas de mitigación o aceptación de riesgos.**
- **Consultar estatus de mitigación, actividades de seguimiento y planificación.**
- **A través de tableros supervise las acciones de implementación y los riesgos gestionados, los que tienen y no tienen acciones de mitigación.**
- **Calcular el riesgo residual.**
- **Presentación de información mediante tableros ejecutivos, mapas de calor y reportes.**
- **Registro y consulta de la actividad realizada por los usuarios mediante pistas de auditoria.**
- **Control de acceso con contraseña robusta de acuerdo con las políticas establecidas.**
- **Apego y cumplimiento con los marcos regulatorios y mejores prácticas como MAAGTICSI, ISO 27001-2, ISO 27032, ISO 31000, NIST, SANS, OWASP.**