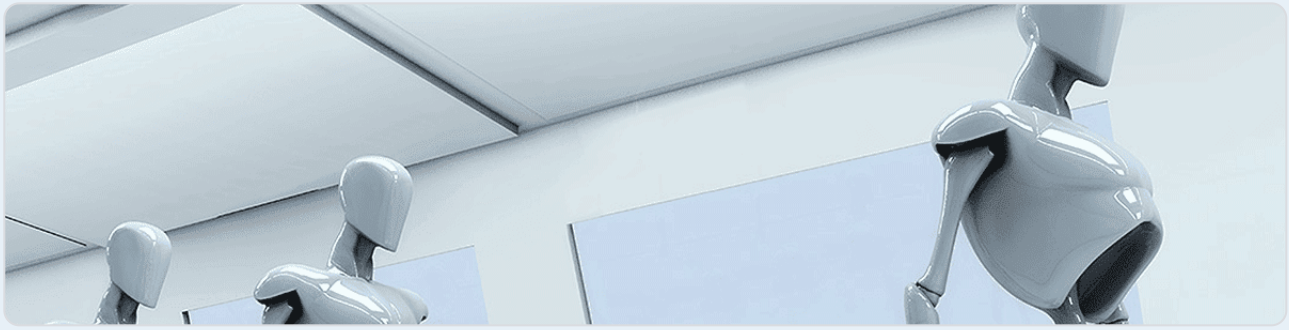


Encuesta de satisfacción del Framework

7 respuestas

Publicar datos de análisis

Datos personales

Nombre completo

7 respuestas

- Eduardo Vilches Romero
- Simón Daniel Miranda Villegas
- -Sebastian Andrès Pinto Lopez
- Patricio Alejandro pereda Fernandez
- Katerine Márceles Villalba
- Sérgio Daniel Fernandes de Oliveira
- Juan Pablo Martínez Pulido

Correo electrónico

7 respuestas

vilchesmeister@gmail.com

smv.77.1993@gmail.com

S.Pinto.López@gmail.com

patricio.pereda@efacec.com

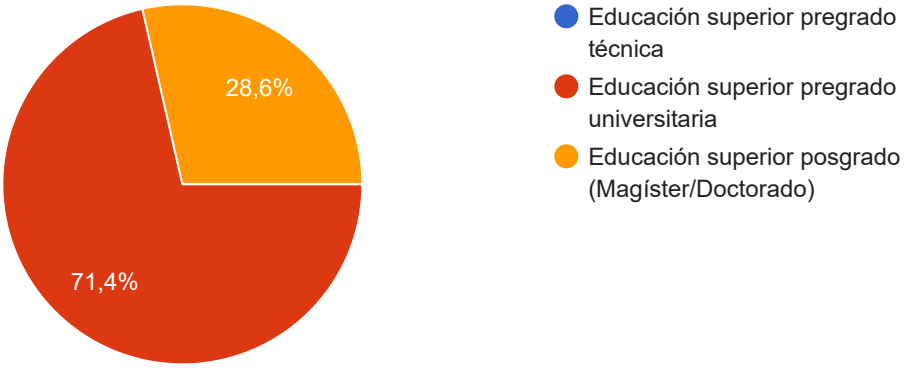
kmarceles@unimayor.edu.co

sergio.fernandes@efacec.com

juanpmartinez@unicauca.edu.co

Nivel de estudios

7 respuestas



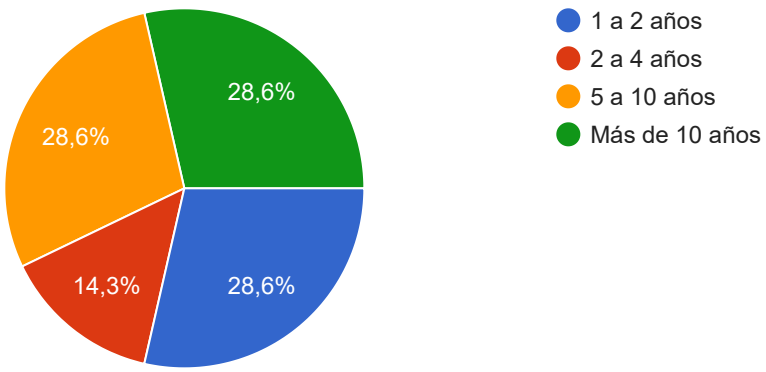
Cargo o función

7 respuestas

- Ingeniero de Servicios
- Ingeniero de servicios
- Ingeniero en servicio
- Gerente comercial
- Docente
- Gerente de Operaciones
- Profesor

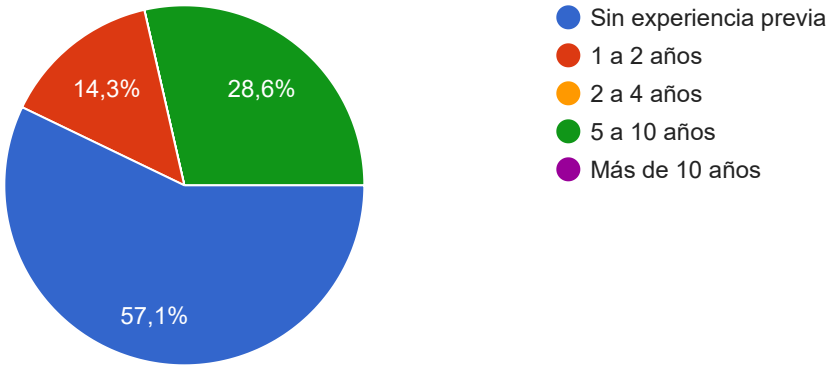
Años de experiencia en trabajo con sistemas SCADA

7 respuestas



Años de experiencia en trabajo con seguridad informática

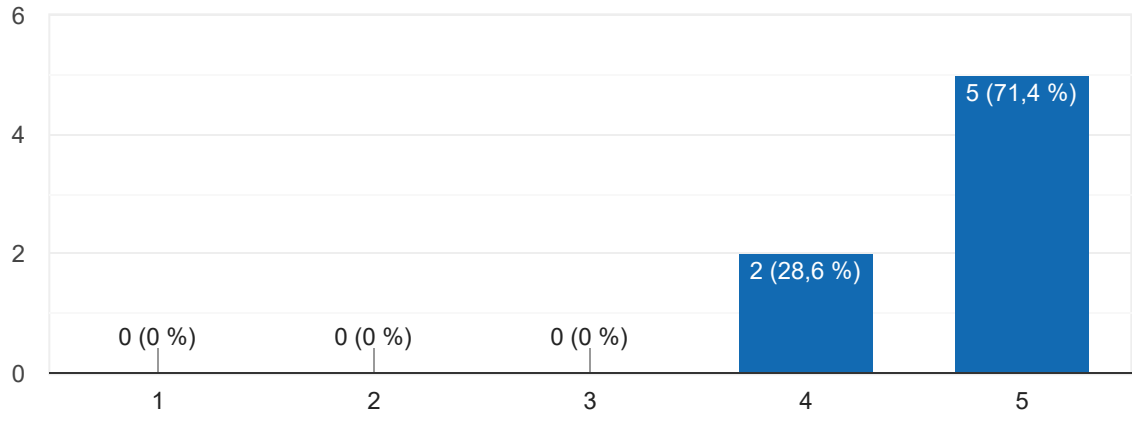
7 respuestas



Preguntas

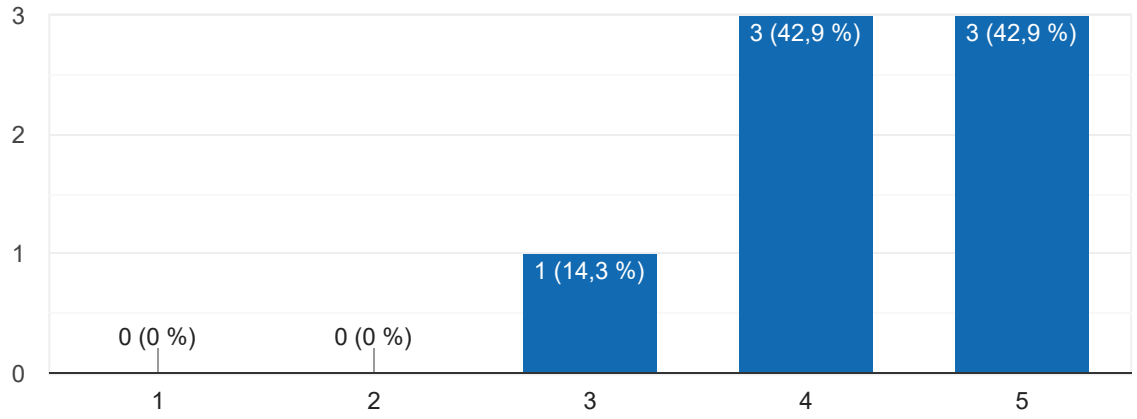
1. Basándose en el hecho que el Framework fue desarrollado utilizando la búsqueda de información en documentos científicos actualizados, metodologías de análisis y explotación de vulnerabilidades con estándares de la industria y experimentación con sistemas reales SCADA UC500 ¿Cree usted que la forma en que fue construido el Framework garantiza que se pueda llevar a cabo el mejoramiento de seguridad de sistemas SCADA?

7 respuestas



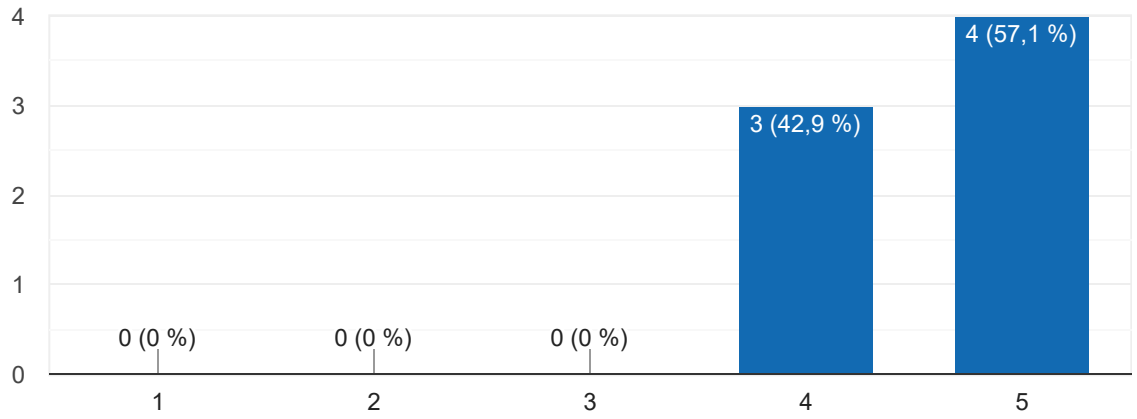
2. Luego de realizar las experimentaciones descritas en el Framework ¿Usted confiaría en esta herramienta para mejorar la seguridad informática de sistemas SCADA actuales y/o futuros?

7 respuestas



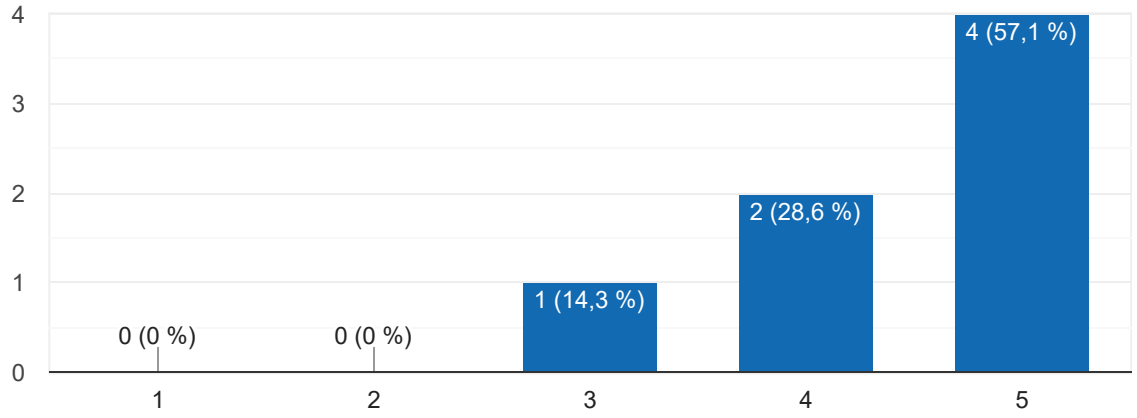
3. La presentación del Framework, fue desarrollada a partir de documentos científicos y experimentación. Respecto a esto ¿La información, redacción, formato, imágenes y tablas expuestos en el Framework, le parecieron consistentes para el entendimiento de seguridad informática en un sistema SCADA?

7 respuestas



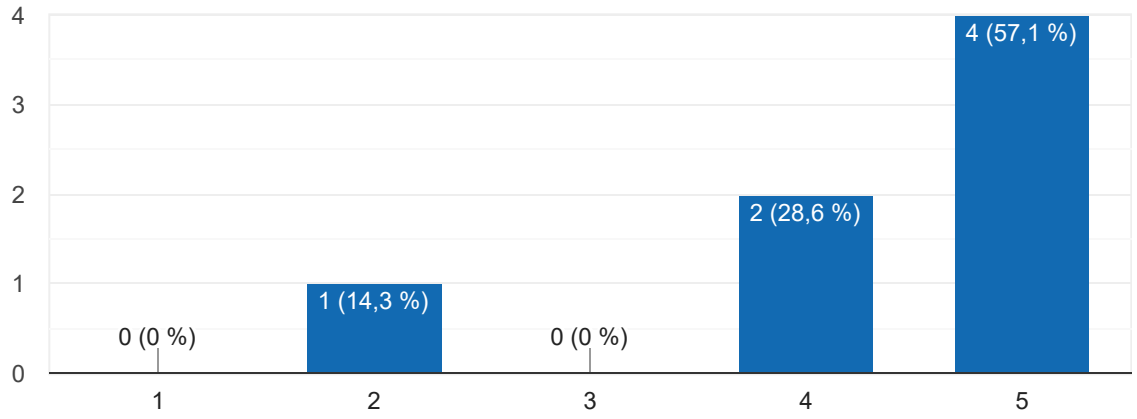
4. ¿Cree usted que el análisis, explotación y mitigación de las vulnerabilidades mostradas en este Framework, aportan a la seguridad informática de los sistemas SCADA?

7 respuestas



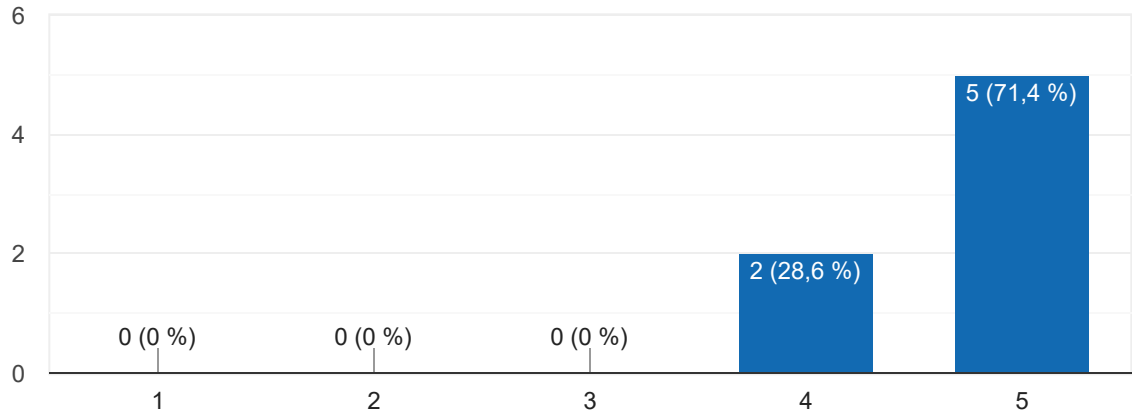
5. Teniendo en cuenta que la calidad de una implementación de un sistema SCADA depende de varios factores, tales como los recursos humanos, tecnológicos, económicos, entre otros. ¿Cree usted que la utilización de herramientas como este Framework, sirven para aportar en mejorar la calidad general en el despliegue de estos sistemas?

7 respuestas



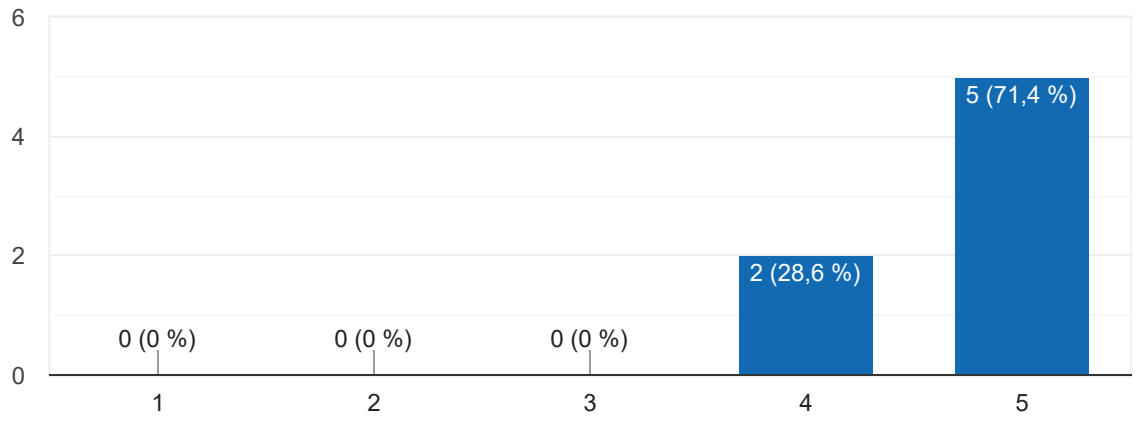
6. ¿Cree usted que los temas, procedimientos y explicaciones expuestos en el Framework, aportaron en su conocimiento respecto a seguridad informática aplicada a sistemas SCADA?

7 respuestas



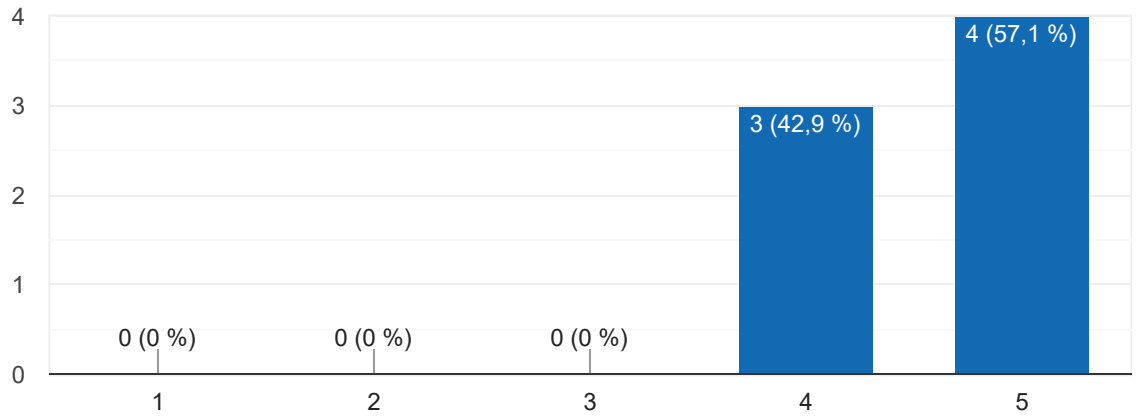
7. ¿Fue precisa y comprensible la información entregada, así como los resultados obtenidos en las pruebas llevadas a cabo aplicando el Framework?

7 respuestas



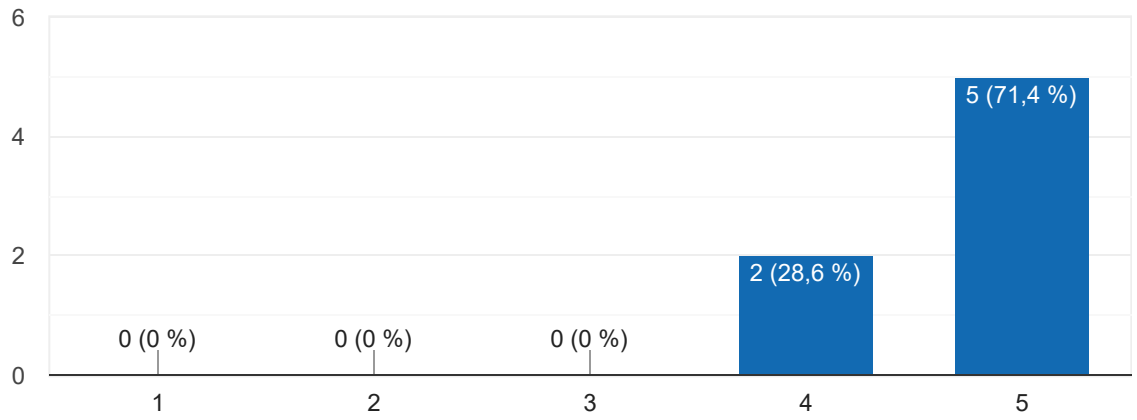
8. ¿Fue fácil para usted implementar las fases propuestas en este Framework?

7 respuestas



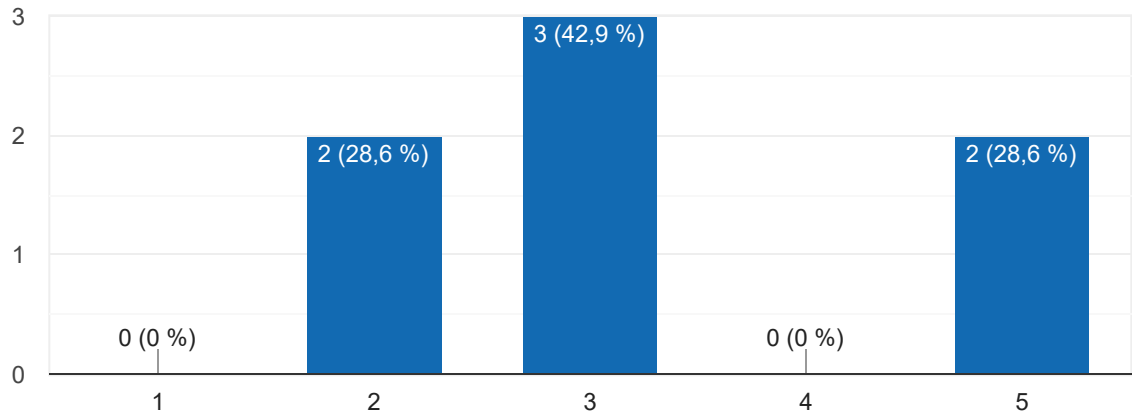
9. ¿Se logró entender la forma de identificación de las vulnerabilidades y las repercusiones que pudieran tener su explotación en un sistema SCADA?

7 respuestas



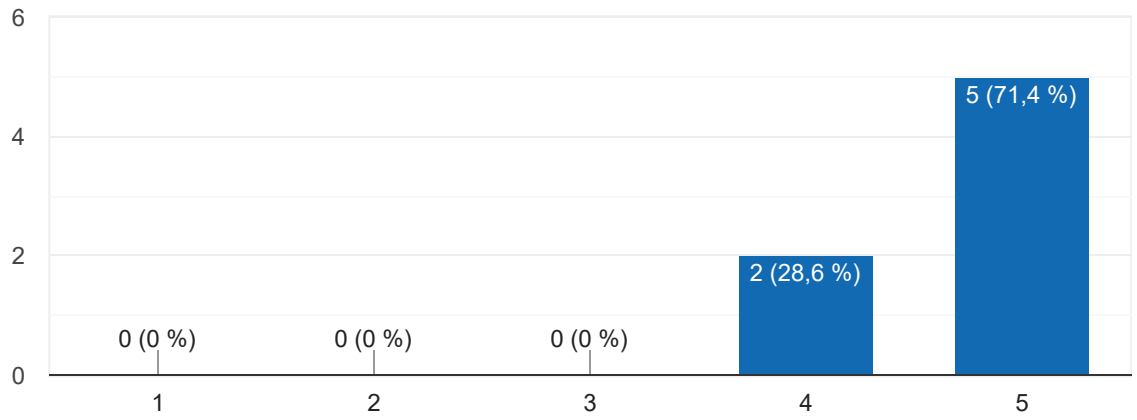
10. ¿Estaba usted familiarizado con conceptos y conocimientos generales en seguridad informática antes de la utilización de este Framework?

7 respuestas



11. ¿Recomendaría a otros profesionales del área relacionados con el diseño, implementación y mantenimiento de sistemas SCADA, la utilización de este Framework?

7 respuestas



12. En esta sección, puede dejar su retroalimentación respecto al Framework de pentesting. Siéntase en la libertad de expresar cual fue su experiencia, lo que más y menos fue de su agrado, así como también sugerencias de mejora en versiones futuras del documento.

6 respuestas

Me sorprendieronz las formas de vulnerar el sistema UC500

El documento presentado entrega conocimiento fundamental, de forma clara y didáctica. Educa de forma transversal, desde personas que dominan el tema a usuarios nuevos, que no necesariamente han estado involucrados con la ciber seguridad de sistemas SCADA anteriormente. Las herramientas entregadas al usuario son gratuitas y se explica de manera ordenada los pasos a seguir para su óptima utilización.

Las pruebas realizadas exhiben con franqueza las vulnerabilidades de los sistemas SCADA Efacec. Necesita un refinamiento importante en diversas áreas, desde las credenciales de acceso, información mostrada innecesariamente (como en los debug de la página misma de acceso) hasta seguridad un poco más avanzada contra ataques como la denegación de servicios (DoS).

En sugerencia de mejora es demasiado especìfica para un sòlo sistema SCADA. Podrìa ser ampliado a diferente sistema y equipos pertenecientes a las Subestaciones.